PART TWO: LOOKING FORWARD

Until now, this report has focused on the limitations and strengths of today's Intelligence Community. We reviewed the Intelligence Community's recent performance in assessing the unconventional weapons programs of Iraq, Libya, and Afghanistan. We also assessed the Intelligence Community's current capabilities to confront several of today's priority intelligence challenges—including Iran, North Korea, and terrorism. (As we have noted elsewhere, while classification concerns precluded us from including our Iran and North Korea findings in our unclassified report, the lessons we learned from these reviews inform our recommendations.) And we complemented the formal "case studies" that appear in Part One of this report with reviews of other important challenges the Intelligence Community faces today, including the need to share intelligence across the Intelligence Community and the difficulties of coordinating intelligence across the foreign-domestic divide.

We found an Intelligence Community that has had some significant successes, but that is, on balance, badly equipped and badly organized to confront today's threats. We found human intelligence collectors who have struggled in vain to find sources with valuable information—and often failed to vet properly the sources they did find. We found technical intelligence collectors whose traditional techniques have declining utility against threats that are increasingly elusive and diffuse. And we found an analytical community too quick to rely upon assumptions or conjecture, and too slow to communicate gaps and uncertainties to policymakers.

But above all, we found an Intelligence Community that was too disorganized and fragmented to use its many talented people and sophisticated tools effectively. There are not enough coordinated and sustained Community-wide efforts to perform critical intelligence functions—ranging from target development to strategic analysis—and critical information still too often does not

get to the analysts or policymakers who need it most. On the flip side of the same coin, we found that many of the Intelligence Community's recent successes stemmed from cross-agency efforts—such as the innovative fusing of different collection capabilities to penetrate a particular intelligence target. We found, in short, an Intelligence Community that needs to be better *integrated* and more *innovative* if it is to be able to confront today's intelligence challenges.

With these lessons in mind, our report now turns toward the future. In the chapters that follow, we set forth our recommendations for change within the Community. We begin our discussion of proposed reforms with a chapter on leadership and management (Chapter 6). However, the task of transforming the Intelligence Community, if it is to be complete, must go beyond questions of organization. As a result, we make recommendations addressing several specific areas of intelligence (or challenges the Intelligence Community faces): Collection (Chapter 7); Analysis (Chapter 8); Information Sharing (Chapter 9); the challenge of uniting intelligence efforts across the foreign and domestic divide (Intelligence at Home, Chapter 10); Counterintelligence (Chapter 11); and a largely classified chapter on managing covert action (Chapter 12). Finally, we conclude with a stand-alone chapter examining our intelligence capabilities with respect to the most dangerous unconventional weapons threats the United States faces today, and offer recommendations on how to improve those capabilities (Proliferation, Chapter 13).

CHAPTER SIX
LEADERSHIP AND MANAGEMENT: FORGING AN INTEGRATED INTELLIGENCE COMMUNITY

Summary & Recommendations

Today's Intelligence Community is not a "community" in any meaningful sense. It is a loose confederation of 15 separate intelligence entities. The new intelligence reform legislation, by creating a Director of National Intelligence (DNI) with substantial new authorities, establishes the basis for the kind of leadership and management necessary to shape a truly integrated Intelligence Community. But the reform act provides merely a framework; the hard work of forging a unified Community lies ahead.

In order to surmount these challenges, the DNI will need to lead the Community; he will need to integrate a diffuse group of intelligence entities by gaining acceptance of common strategic objectives, and by pursuing those objectives with more modern management techniques and governance processes. In this chapter we recommend several structures that could demonstrate the value of such collaboration.

Specifically, we recommend that the DNI:

- Bring a mission focus to the management of Community resources for high-priority intelligence issues by creating several "Mission Managers" on the DNI staff who are responsible for overseeing all aspects of intelligence relating to priority targets;
- Create a leadership structure within the Office of the DNI that manages the intelligence collection process on a Community basis, while maintaining intact existing collection agencies and their respective pockets of expertise;
- Make several changes to the Intelligence Community's personnel policies, including creating a central Intelligence Community human resources authority; developing more comprehensive and creative sets of performance incentives; directing a "joint" personnel rotation system; and establishing a National Intelligence University.

Summary & Recommendations (Continued)

We also recommend that:

- The President establish a National Counter Proliferation Center (NCPC) that reports to the DNI. The NCPC—a relatively small organization, with approximately 100 staff—would manage and coordinate analysis and collection on nuclear, biological, and chemical weapons across the Intelligence Community, but would not serve as a focal point for government-wide strategic operational planning; and
- The Executive Branch take steps to strengthen its intelligence oversight to ensure that intelligence reform does not falter, and that the Intelligence Community strengthen its own processes for self-evaluation.

INTRODUCTION

Today's Intelligence Community is not truly a community at all, but rather a loose confederation of 15 separate entities.[1] These entities too often act independently of each other. While a "community" management staff has long existed in the Office of the Director of Central Intelligence (DCI), it has never had the authority or resources it needed to manage all these disparate components.

The diffuse nature of the Intelligence Community does have important merits—for example, the existence of different agency cultures and ways of doing business increases the likelihood that hypotheses about key intelligence issues will be "competitively" tested, and allows for the development of diverse pockets of expertise. While such advantages should be retained, they aren't a reason to tolerate the current lack of coordination. As our case studies aptly demonstrate, the old, single-agency methods of gathering intelligence are losing ground to our adversaries. And conversely, many of our recent intelligence successes have resulted from innovative cross-agency efforts—but such laudable examples are the exception, the products of *ad hoc* efforts rather than institutionalized collaboration.

Concern about the harmful impact of disunity on national security was a major factor leading to passage of the *Intelligence Reform and Terrorism Prevention Act of 2004*. In creating a Director of National Intelligence (DNI) with

substantial (though not sweeping) new authorities, the act created the framework for an integrated management structure for the United States' intelligence apparatus. However, passage of the intelligence act is merely prologue; the hard work of forging a genuine Intelligence Community, linked for the purpose of optimizing its capabilities and resources, must now begin.

We are realists. We recognize that effecting such a transformation in intelligence will take years to accomplish—and, indeed, will fall short without sustained leadership from the Director of National Intelligence and continued support from the President and Congress. This chapter offers our view on the essential tasks the new DNI might prioritize—and the challenges he will confront—as he begins this effort. We also offer, at the end of the chapter, a notional organizational structure for the new Office of the DNI, which we believe would serve the DNI well in confronting these tasks and challenges.

BUILDING AN INTEGRATED INTELLIGENCE COMMUNITY

Levers of Authority: Powers and Limitations of the New DNI

First, the good news. Under prior law, the Director of Central Intelligence had three demanding jobs—he ran the CIA, acted as the President's principal intelligence advisor, and (in theory, at least) managed the Intelligence Community. Thanks to the new intelligence legislation, the new DNI is now only responsible for two; the task of running the day-to-day operations of the CIA will be left to the Agency's own Director.[2]

The bad news is that the DNI's remaining statutory responsibilities continue to be demanding, full-time jobs. The DNI's management responsibilities will be both critically important and exceedingly difficult, and there is a real risk that the obligation to provide current intelligence support to the President and senior policymakers will reduce or eliminate the attention the DNI can devote to the painstaking, long-term work of integrating and managing the Community. It would be unrealistic—and undesirable—to expect the Office of the DNI to neglect or abdicate its responsibility as intelligence advisor to the President. But it is not necessary in all instances for the DNI to be present at the briefings himself. We do believe that it is possible for the DNI to assume what is essentially an oversight rather than a direct role in fulfilling this function, and we suggest that the DNI interpret the obligation in this way.

The DNI's management responsibilities will be more than sufficient to occupy the DNI's time and talents. On the first day in office, the new DNI will not have much of a foundation to build upon. A former senior Defense Department official has described today's Intelligence Community as "not so much poorly managed as unmanaged."[3] After a comprehensive study of the Community, we can't disagree. The DNI will need to create—virtually from scratch—structures, processes, and procedures for managing this notoriously sprawling, complicated, and fragmented bureaucracy. But with this "blank slate" also comes an opportunity. The new Director will be in a position to build a leadership and management staff that is suited to today's intelligence needs, rather than accommodate and modify an inherited administrative structure.

The intelligence reform legislation gives the DNI substantial new levers of authority to perform management responsibilities, but those powers are also limited in important respects. Most of the entities within the Intelligence Community—such as NSA, NGA, and the intelligence component of the FBI—continue to be part of separate executive departments. This means that the DNI will be expected to manage the Intelligence Community, but will not have direct "line" authority over all the agencies and entities he is responsible for coordinating and integrating. NSA, to cite just one example, remains with the Department of Defense, and its employees will therefore continue to be part of the Defense Department's "chain of command."

This means that the DNI will be required to manage the Community more by controlling essential resources than by command. And the new legislation does give the DNI important new budget and personnel authorities. For example, the intelligence reform act grants the DNI a substantially stronger hand in the development and execution of the overall intelligence budget, or National Intelligence Program, than that previously given to the DCI.[4] The leverage that these budget authorities were intended to provide, however, cannot be effectively exercised without an overhaul of the Intelligence Community's notoriously opaque budget process, which obscures how resources are committed to, and spent against, various intelligence programs. The DNI could wield his budgetary authorities with far more effectiveness if he were to build an end-to-end budgetary process that allowed for clarity and accountability—a process similar to the Planning, Programming, and Budgeting System employed by the Department of Defense.

With that said, the DNI's "power of the purse" is far from absolute. Many important intelligence programs are funded in whole or in part from joint military and tactical intelligence budgets that are under the control of the Defense Department.[5] In light of these overlapping responsibilities and competing budgetary authorities, it is imperative that the Office of the DNI and the Department of Defense develop parallel and closely coordinated planning, programming, and budget processes. (Indeed, the relationship between the DNI and the Secretary of Defense is of great importance and will be discussed separately in this chapter.)

Another important (and related) management tool for the DNI is the acquisition process. If the DNI builds and drives a coherent, top-down Intelligence Community acquisition structure, he will have a powerful device for Community management, and will make an important step toward developing the coherent long-term allocation of resources that the Intelligence Community sorely lacks today—particularly with respect to evaluating and acquiring large, technology-driven systems. But, as in other areas, the DNI's role in the acquisition process is not absolute. Under the new intelligence reform act, the Secretary of Defense and the DNI will have joint acquisition authorities in many instances—another factor that weighs in favor of strong Defense Department-Intelligence Community interaction on many fronts.[6]

In addition to these budget and acquisition authorities, the intelligence act also grants the DNI significant personnel powers. The act gives the DNI a substantial staff, and it empowers the DNI to transfer personnel from one element of the Intelligence Community to another for tours of up to two years.[7] These are important new authorities; our terrorism case study sets out the difficulties the Terrorist Threat Integration Center encountered in obtaining adequate personnel support from other agencies. However, like the DNI's budgetary authorities, these powers are not unrestricted; the intelligence reform act states that the procedures governing these personnel transfers must be developed jointly by the DNI and by the affected agencies,[8] which could provide department and agency heads with an opportunity to impede the DNI's initiatives. We suggest that the DNI make the development of these procedures an early priority, to ensure that the required "procedures" become just that—processes for effecting the flexible transfer of personnel and minimizing negative impact on the affected agencies, and not vehicles that provide agencies with a veto over the DNI's personnel authorities.

The intelligence act also expressly directs the DNI to implement management-related reform measures that have long been neglected by Community managers. Among these are specific mandates to develop Community personnel policies; maximize the sharing of information among Community agencies; improve the quality of intelligence analysis; protect the sources and methods used to collect intelligence from disclosure; and improve operational coordination between CIA and the Department of Defense. This explicit congressional direction should significantly strengthen the DNI's hand as the work of creating a new management structure begins.

The DNI will likely need every bit of the leverage bestowed by these new powers and embodied in the statutory mandate for change. Few of the recommendations that follow can be implemented without affecting the current responsibilities of a particular agency, sometimes in ways that can be expected to leave the affected agency unhappy. For instance, if the DNI is going to manage the target development system—the process by which the Intelligence Community prioritizes information needs and develops collection strategies to fulfill those needs—he will, by necessity, be taking responsibilities away from the collection agencies. If the DNI is going to build a modern information sharing infrastructure for the Intelligence Community, he will need to override particular agencies' views about what information is and is not too sensitive to be placed in the shared information space.

Making hard decisions that adversely affect particular agencies will constitute a major departure from prior Community management practices. Former DCIs have brought the Intelligence Community together by consensus, a practice that left many difficult but important management challenges unaddressed. Indeed, over the course of our study we repeatedly came across important decisions that Community leaders were unable to resolve—a state of affairs that allows bureaucratic disputes and unhealthy ambiguities in responsibilities to fester. (The lengthy turf battle between the CIA Counterterrorist Center and the Terrorist Threat Integration Center (now NCTC), which we discussed in Chapter Four (Terrorism), is just one example.)

While the air is thick with talk of the need for coordination within the Intelligence Community, one can expect that the DNI's new (and sometimes ambiguous) authorities will be challenged in ways both open and subtle. In order to sustain successful integration, the DNI will need to establish processes that demonstrate by their own effectiveness the value of Community-

wide cooperation. This can be achieved by securing "buy-in" on common strategic objectives, developing common practices in reviewing progress toward goals (using shared metrics whenever possible), and building a common approach to human resource management. We recommend several structures—such as the "Mission Managers" that we discuss immediately below—that could be useful in demonstrating the value of collaboration, and we also encourage the DNI to seek to emulate best practices used by large organizations both within and outside government.

Organize Around Missions

Throughout our study, we observed a lack of Community focus on intelligence missions. Each individual agency tries to allocate its scarce resources in a way that seems sensible to that particular agency, but might not be optimal if viewed from a Community perspective. The DCI's management staff is organized around intelligence functions—there are, for instance, separate Assistant DCIs for "Collection" and "Analysis"—rather than around priority intelligence targets. So while it might have been the case that an individual at the DCI level was responsible for knowing about our collection capabilities on a given country, and while it might also have been the case that an individual at the DCI level was responsible for knowing the state of *analysis* on that country, no one person or office at the DCI level was responsible for the *intelligence mission* concerning that country as a whole.

We believe it is important that the DNI develop a management structure and processes that ensure a strategic, Community focus on priority intelligence missions. The specific device we propose is the creation of "Mission Managers."

Recommendation 1

We recommend that the DNI bring a mission focus to the management of Community resources for high-priority intelligence issues by creating a group of "Mission Managers" on the DNI staff, responsible for all aspects of the intelligence process relating to those issues.

Under the current system, collectors, analysts, and supervisors throughout the Community working on a given target function largely autonomously, communicating and collaborating only episodically. The Mission Managers we propose would be responsible for designing and implementing a coordinated

effort. As the DNI's point person for individual high-priority subject matter areas, Mission Managers would be responsible for knowing both what the Community knows (and what it does not know) about a particular target, and for developing strategies to optimize the Community's capabilities against that particular target. For any such target—be it a country like China, a non-state actor like al-Qa'ida, or a subject like "proliferation"— a Mission Manager would be charged with organizing and monitoring the Community's efforts, and serving as the DNI's principal advisor on the subject. Most importantly, and in contrast to the diffusion of responsibility that characterizes the current system, the Mission Manager would be the person *responsible* for Community efforts against the target. There would never be a question of accountability.

The Mission Manager, therefore, would have substantial responsibilities both for driving collection and identifying shortcomings in analysis in the Mission Manager's subject area. With respect to collection, Mission Managers would chair Target Development Boards, described further below and in Chapter Seven (Collection). In this capacity, the Mission Managers' role would include identifying collection gaps, working with the various collection agencies to fill them, and monitoring the collection organizations' progress in that regard. As explained in greater detail in Chapter Eight (Analysis), they would also serve as the DNI's primary tool for focusing the Intelligence Community's analytical attention on strategic threats to national security and optimizing the Community's resources against them. While they would not directly command the analytical cadre, they could—in cases where agency heads were resistant to properly aligning resources or addressing analytic needs—recommend that the DNI's personnel powers be invoked to correct the situation or quickly re-configure the Community to respond to a crisis. Because of their responsibilities for developing a coordinated approach to collection and analytic efforts, we believe that the Mission Managers would also collectively serve as an important device for achieving Community integration over time.[9]

Some might suggest that the Mission Manager function will conflict with the role of National Intelligence Officers (NIOs) within the National Intelligence Council (NIC), the Community's focal point for long-term, interagency analysis. The NIOs are granted authority under the new legislation for "evaluating community-wide collection and production of intelligence by the Intelligence Community and the requirements and resources of such collection and production."[10] We believe this role is complementary with that of the Mission

Managers. NIOs, in our view, should continue to serve as the Community's principal senior analysts. In this position, they spearhead assembly of National Intelligence Estimates and other publications that articulate Community analytic conclusions, identify differences in agency views and why they exist, and explore gaps and weaknesses in collection. But once an Estimate on a given topic is finished, NIOs move quickly to the next, perhaps not to officially revisit the subject matter for years. They have neither the time nor the authority to craft and implement strategic plans designed to improve the Community's work on a particular issue over time. This, as we see it, will be the Mission Managers' role.

Coordinate Target Development

Recommendation 2

We recommend that the DNI create a management structure that effectively coordinates Community target development. This new target development process would be supported by an integrated, end-to-end "collection enterprise."

The Intelligence Community's fragmented nature is perhaps best exemplified by the process in which its resources are directed to collect information on subjects of interest. One would expect that this vital aspect of intelligence—which we refer to as "target development"—would be among those where coordination and integration is most essential. Instead, the target development process is left primarily to individual collection agencies, operating from a general list of intelligence objectives called the National Intelligence Priorities Framework, in combination with *ad hoc* requirements generated by analysts and other intelligence "customers," such as policymakers and the military. This decentralized process is refined only episodically at the Community level, usually through the personal intervention of the Assistant Director of Central Intelligence for Collection.

This is an unacceptable status quo, and we recommend that the DNI make fixing it a top priority. As our case studies have shown, many of the recent penetrations of hard targets have been facilitated by fusing collection disciplines. Such cross-agency collection strategies cannot be systematically encouraged while the various collection platforms remain isolated within the confines of their individual agencies. The current system, in which individual agencies set

their own collection priorities, also marginalizes the role of the intelligence "customers" and analysts for whom intelligence is collected.

As a result, we believe it is essential that the DNI develop a unified target development process that exists "above the stovepipes." We develop more fully our target development recommendations in Chapter Seven (Collection), but because of the importance of this issue we highlight it here. We would give the Mission Managers responsibility for driving and maintaining an overarching collection strategy in their subject matter areas. In developing this strategy, each Mission Manager would chair, and be supported by, a standing DNI-level Target Development Board that would include experts from key "customers" and from each major collection agency, who could keep the Mission Manager informed of its agency's capabilities (and limitations) against the target. This approach would ensure that the target development process was both integrated and user-driven.

We also recommend that the target development process be supported by an integrated "collection enterprise": that is, a collection process that is coordinated and integrated at all stages, from collection management to data exploitation to strategic investment. Again, we discuss this recommendation in detail in Chapter Seven (Collection).

Facilitate Information Sharing

Recommendation 3

We recommend that the new DNI overhaul the Community's information management system to facilitate real and effective information sharing.

No shortcoming of the Intelligence Community has received more attention since the September 11 attacks than the failure to share information. There have been literally dozens of Intelligence Community initiatives in this area, with advances most apparent in the area of counterterrorism. Unfortunately, almost all of these efforts have worked around the most intractable and difficult information-sharing impediments, rather than solved them. While minor advances have been made in some areas, the ultimate objective of developing a Community-wide space for sharing intelligence information has proven elusive. In our view, the fundamental reason for the lack of suc-

cess is the absence of empowered, coherent, and determined Community leadership and management.

We strongly recommend that the new DNI tackle this problem early on by overhauling the Community's information management system, including as a central component the creation of a single office responsible both for information management and information security. We also suggest that the DNI begin with a painless, but symbolically important, first step: namely, to jettison the very phrase "information sharing." To say that we must encourage agencies to "share" information implies that they have some ownership stake in it—an implication based on a fundamental (and, unfortunately, all too common) misunderstanding of individual collection agencies' obligations to the Intelligence Community, and to the government more broadly. We believe that the DNI might begin the process of building a shared information space by putting the DNI's imprimatur on a new phrase, perhaps "information access," that indicates that information within the Community is a Community asset—not the property of a particular agency. Our information sharing recommendations, which we detail in Chapter Nine (Information Sharing), begin from this premise.

Create Real "Jointness" and Build a Modern Workforce

Recommendation 4

We recommend that the DNI use his human resources authorities to: establish a central human resources authority for the Intelligence Community; create a uniform system for performance evaluations and compensation; develop a more comprehensive and creative set of performance incentives; direct a "joint" personnel rotation system; and establish a National Intelligence University.

Perhaps the most effective authorities the intelligence reform act grants the DNI are those pertaining to personnel. These new authorities come none too soon, as it is becoming increasingly apparent that the Intelligence Community cannot continue to manage its personnel system the way it always has. The Community still attracts large numbers of highly qualified people, but retaining them has become a real challenge. Today's most talented young people change jobs and careers frequently, are famously impatient with bureaucratic and inflexible work environments, and can often earn far more outside the government. The Community's personnel system is ill-suited to hire and

retain people with these characteristics; merely getting hired can take over a year, and compensation is too often tied to time-in-grade, rather than demonstrated achievement.

Moreover, at precisely the moment when the Intelligence Community is facing the prospect of recruiting in this very different job market, the average experience level of the people in many elements of the Intelligence Community is declining. It is uncertain whether this is merely a transitory phenomenon, reflecting an ambitious post-9/11 hiring program. The analytical cadre may grow in experience and stabilize over the next few years. In the short term, however, it is clear that the Intelligence Community suffers from an eroding base of institutional wisdom, not to mention a lack of accumulated knowledge and expertise.

These overarching employment trends are, unfortunately, only the tip of the iceberg. Today's Intelligence Community has additional systemic weaknesses with regard to personnel. For example, the Community has had difficulty recruiting individuals with certain critical skill sets; has often failed to encourage the type of "joint" personnel assignments that are necessary to breaking down cultural barriers that exist among agencies; and has proven insufficiently adept at hiring and mainstreaming mid-career "lateral" hires from outside of the Intelligence Community. This section suggests reforms of the human resources system that would help equip the Community to confront these formidable challenges.

Establish a central Human Resources Authority for the Intelligence Community. As a threshold matter, the Intelligence Community needs a DNI-level office responsible for analyzing the workforce, developing strategies to ensure that priority intelligence missions are adequately resourced, and creating Community human resources standards and policies to accomplish these objectives. The human resources authority would also establish evaluation standards and metrics programs to assess the intelligence agencies' performance in hiring, retention, and career development.

This office would also have responsibility for developing policies to fill gaps in the Intelligence Community's workforce. Our case studies have highlighted a wide variety of these critical personnel needs. We have found that the Community has difficulty in attracting and retaining people with scientific and technical skills, diverse ethnic and religious backgrounds, management experience,

and advanced language capabilities. Similarly, the Community has struggled to develop the mid-career lateral hires that will be increasingly necessary to complement a workforce that can no longer expect to depend on Intelligence Community "lifers." This authority would have responsibility for developing the Community personnel policies that can overcome these systemic shortcomings.

Direct a personnel rotation system that develops "joint" professionals in the senior ranks of the Intelligence Community. Much has been made of the need to develop "jointness" in the Intelligence Community. Study after study has cited the significance of the Goldwater-Nichols Act in transforming the U.S. military from four independent services to a single, unified fighting force.[11] The Goldwater-Nichols analogy does not apply perfectly to the Intelligence Community; as we discuss below, we do not believe that the Intelligence Community should be reorganized comprehensively around national intelligence "centers" that would serve as the equivalent to the military's joint commands. But we do believe that the personnel reforms of the Goldwater-Nichols Act, which encouraged (and in some instances required) individuals to serve "joint" tours of duty outside of their home services, should be replicated within the Intelligence Community.

We recommend, therefore, that the DNI promptly develop mechanisms to ensure that joint assignments are taken seriously within the Intelligence Community. Today, the Community's agencies vary substantially in the seriousness of their commitment to cross- and interagency assignments. It is insufficient merely to ensure that an Intelligence Community professional who works in an Intelligence Community center or at a different intelligence agency will suffer no punishment upon returning home. Instead, personnel should be affirmatively rewarded for successfully completing joint tours, and intelligence professionals should gain eligibility for promotion to senior levels only if they complete joint assignments. Jointness did not occur effortlessly in the Department of Defense. The DNI will likely find that fostering a truly "joint" culture in the Intelligence Community will require significant and persistent attention.

Create more uniform performance evaluation and compensation systems. Personnel systems across the Intelligence Community are in flux, with some agencies moving to new merit-based pay systems and others retaining but modifying the traditional federal General Schedule (GS) system. These differences

have the effect of inhibiting the cross-agency movement of personnel that is so critical to building an integrated Intelligence Community. To avoid this problem, we recommend that the Intelligence Community's human resources authority adopt a common personnel performance evaluation and compensation plan. This plan would define core Community competencies and set evaluation criteria (for the entire workforce as well as for key segments, such as analysts), and establish a standard pay grade and compensation structure—while retaining the flexibility to allow agencies to evaluate performance factors unique to their organizations. We further recommend that such a unified compensation structure be based on a merit-based model. A merit-based approach is being used increasingly across the federal workforce, and more rationally links performance to organizational goals and strategies.

We also believe that this review of the compensation structure should focus in particular on ways for the Intelligence Community to recruit talented individuals from *outside* the government. Today, the Intelligence Community can promise the following to talented scientists, scholars, or businesspersons who wish to serve: a lengthy clearance process before they begin, a large pay and benefits cut, a work environment that has difficulty understanding or using the talents of outsiders, and ethics rules that significantly handcuff them from using their expertise when they seek to return to their chosen professions. It should come as little surprise that too few talented people from the private sector take the offer. The DNI should develop special hiring rules aimed at attracting such individuals, including special salary levels and benefits packages and streamlined clearance processes.

Develop a stronger incentive structure within the Intelligence Community. In addition to encouraging greater use of financial incentives, we recommend that the Community consider new techniques to motivate positive performance. A real "Intelligence Community" would reward and encourage types of behaviors that currently are not emphasized. These behaviors—a commitment to sharing information, a willingness to take risk, enthusiasm for collaborating with intelligence professionals at other agencies, and a sense of loyalty to the Intelligence Community's missions—must be reinforced if they are to become institutionalized. Government entities are severely limited in the monetary rewards they can offer to reinforce desired behavior, but there are other rewards that can serve as suitable alternatives. Advanced education and training, professional familiarization tours, coveted assignments, and

opportunities to attend conferences and symposia are all rewards that might be associated with reinforcing new behaviors.

But it is not enough merely to encourage the right kinds of behavior; it is also critical that the Intelligence Community does not reward its employees for the wrong reasons. Our review found that agencies within the Intelligence Community often made personnel decisions based upon the wrong criteria. For instance, as discussed in our Iraq case study, agencies that collect human intelligence place considerable value on the number of sources they recruit—an incentive system that of course encourages its employees to recruit easier, less important sources rather than taking the time (and the risk) to develop the harder ones. A similar problem exists in the analytical community, where we were told that analysts are disproportionately rewarded for producing "current intelligence" assessments, such as articles that appear in the President's Daily Brief. If we are to expect our human intelligence collectors to take risks and our intelligence analysts to devote time to long-term, strategic thinking, agencies must have a personnel evaluation system that does not punish them for these behaviors.

Establish a National Intelligence University. The Intelligence Community has a number of well-founded and successful training programs. Individual organizations within the Community conduct various discipline-specific training programs.[12] Yet there is no initial training provided to all incoming Intelligence Community personnel that instills a sense of community and shared mission—as occurs, for example, in all of the military services. Nor is there an adequate management training program[13]—a fact that may have contributed to declining numbers in the Intelligence Community's mid-level management corps, and the low performance evaluations that this corps recently received in one major intelligence agency.

A National Intelligence University (NIU) could fill these gaps by providing Community training and education programs, setting curriculum standards, and facilitating the sharing of the Community's training resources. A progressive and structured curriculum—from entry level job-skills training to advanced education—could link to career-advancement standards for various Intelligence Community occupations and permit intelligence professionals to build skills methodically as they advance in their responsibilities. The NIU could also serve as a research center for innovative intelligence tools and a test bed for their implementation across the Intelligence Community. The

development of such a university—which could be built easily and at modest expense on top of existing Intelligence Community training infrastructure—would be a relatively easy and cost-effective way to develop improved Community integration and professionalism.

Develop New Mechanisms for Spurring Innovation

Recommendation 5

We recommend that the DNI take an active role in equipping the Intelligence Community to develop new technologies.

While human intelligence has always been the most romanticized of the collection disciplines, technology has driven the course of intelligence over the past century. Advanced technology and its creative application remain a comparative advantage for the United States, but we fear that the Intelligence Community is not adequately leveraging this advantage. Elements of the Intelligence Community continue to perform remarkable technical feats, but across many dimensions, Intelligence Community technology is no longer on the cutting edge. And this problem affects not only intelligence collection; we also lag in the use of technologies to support analysis. This trend may result from a recent decline in the Intelligence Community's commitment to scientific and technological research and development.

We advise the DNI to take an active role in reversing this trend. To be sure, individual agencies will continue to develop new technologies that will serve their missions. But we recommend that the DNI encourage a parallel commitment to early-stage research and development to ensure that important new technologies that might be neglected by individual collection agencies are explored. Toward this end, we recommend that the Office of the DNI have its own significant pool of research and development money at its disposal.

It is not enough, moreover, merely to develop new technologies; it is also critical to ensure that there are effective processes in place to make sure those new technologies are actually put into practice. Like many large organizations, the Intelligence Community has had difficulty "mainstreaming" new technologies (which are often developed by outside organizations like In-Q-Tel, a private, non-profit entity that identifies and invests in new technologies for the CIA). It also often fails to build programmed funding transitions from

research and development to deployment. In order to ensure that new technologies actually reach the users who need them, we recommend that the DNI require the larger agencies within the Intelligence Community to establish mechanisms for integrating new technologies, and develop metrics for evaluating each agency's performance in this regard.

In Chapter Seven (Collection), we recommend DNI-level management practices that would encourage the development of new technical collection technologies. But there is more to the problem than that. Research and development leaders within the Intelligence Community have told us that they cannot attract or retain the best and the brightest young scientists and engineers because career paths are unattractive, the Community's research infrastructure is poor, and the environment is too risk averse. We have seen similar shortfalls in technical and scientific expertise among the analytic corps and within the cadre of human intelligence collectors. As has been noted above, we advise the DNI to utilize personnel authorities to ensure that scientific and technical career tracks are adequately developed and rewarded by intelligence agencies.

A DIFFERENT KIND OF "CENTER": DEVELOPING THE NATIONAL COUNTER PROLIFERATION CENTER

Recommendation 6

We recommend that the President establish a National Counter Proliferation Center (NCPC) that is relatively small (*i.e.*, fewer than 100 people) and that manages and coordinates analysis and collection on nuclear, biological, and chemical weapons across the Intelligence Community. Although government-wide "strategic operational planning" is clearly required to confront proliferation threats, we advise that such planning *not* be directed by the NCPC.

In the preceding section we recommended that the new Director of National Intelligence take several steps aimed at forging a better integrated Intelligence Community. In this section we address whether this objective could be further advanced through the creation of a National Counter Proliferation Center (NCPC). The recent intelligence reform legislation envisions the creation of an NCPC modeled on the newly-created National Counterterrorism Center

(NCTC).[14] But the act also gives the President the opportunity to decide not to create the center—or to modify certain characteristics—if the President believes that doing so serves the nation's security.[15]

Although we endorse the idea of creating an NCPC, we believe it should look very different from the NCTC. The distinguishing feature of the NCTC is its hybrid character: the NCTC serves simultaneously as an integrated center for counterterrorism intelligence *analysis* and as a driver and coordinator of national interagency counterterrorism *policy* (the new intelligence legislation describes this latter responsibility, in rather confusing fashion, as "strategic operational planning"). As a result of these two roles, the Director of the NCTC has a dual-reporting relationship; he reports to the DNI on terrorism intelligence matters, and reports to the President when wearing his policy coordination hat. While we understand the motivations that may have led to these overlapping intelligence and policy functions in the counterterrorism area, we doubt that it is a good idea to replicate the model—and the mixed reporting relationships it creates—in other substantive areas.

We are also skeptical more generally about the increasingly popular idea of creating a network of "centers" organized around priority national intelligence problems. While we sympathize with the desire for better coordination that animates these proposals, centers also impose costs that often go unappreciated. As our Iraq case study aptly illustrates, centers run the risk of crowding out competitive analysis, creating new substantive "stovepipes" organized around issues, engendering turf wars over where a given center's mission begins and ends, and creating deeply rooted bureaucracies built around what may be temporary intelligence priorities. In most instances we believe that there are more flexible institutional solutions than centers, such as the national Mission Managers we propose.

So, while we recommend the creation of a National Counter Proliferation Center, the center we envision would differ substantially from both the NCTC and from the large analytical centers that some have suggested might serve as organizing units for the Intelligence Community. The NCPC we propose would serve as the DNI's Mission Manager on counterproliferation issues: it would not conduct analysis itself, but would instead be responsible for *coordinating* analysis and collection on nuclear, biological, and chemical weapons[16] across the Intelligence Community. As such, it would be much smaller than the NCTC (it would likely require a staff of no more than 100 people) and

would not perform a policy planning function. Specifically, the Director of the NCPC would:

Develop strategies for collecting intelligence on the proliferation of nuclear, biological, and chemical weapons (and their delivery vehicles). The Director of the NCPC would manage the target-development process for nuclear, biological, and chemical weapons. Like any Mission Manager, the NCPC would develop multi-disciplinary collection strategies to attack hard targets, and would review the performance of collection agencies in gaining access to these targets. Similarly, it would have full visibility into all compartmented intelligence programs, thus ensuring that relevant capabilities are fully employed by collectors and considered by analysts.

Coordinate, oversee, and evaluate analytic production. As already noted—and in contrast to the National Counterterrorism Center—the NCPC would *not* contain a large staff of analysts working on proliferation. Rather, the NCPC would coordinate decentralized analytic efforts occurring at various agencies. This would increase the likelihood of competitive analysis of proliferation issues across the Community. In some cases, the NCPC might determine that no part of the Community is addressing a proliferation-related issue sufficiently and designate a small group of resident NCPC analysts drawn from throughout the Community to work on the issue.

With these analytic oversight responsibilities, the NCPC will fulfill several critical functions, including ensuring that appropriate technical expertise is focused on state weapons programs; that gaps in the Community's knowledge about the relationship between state actors and non-state threats (*e.g.*, black- and gray-market proliferators such as A.Q. Khan) are addressed; and that the NCTC has access to subject matter expertise on nuclear, biological, and chemical questions. We do not believe that the NCPC should take the lead on the crucial question of the terrorist procurement of unconventional weapons. That responsibility should, in our view, fall to the NCTC. But the Director of the NCPC should support the NCTC and be prepared to step in and appeal to the DNI if this crucial area is receiving insufficient resources and attention.

Participate in setting the budget associated with nuclear, biological, and chemical weapons. As the 9/11 Commission correctly noted, true management authority also must include some budget authority.[17] In line with this observation, the NCPC would make recommendations regarding counterpro-

liferation-related budget submissions for National Intelligence Program funds. The NCPC would also support the DNI in fulfilling his statutory responsibilities to "participate" in the development of counterproliferation-related program funds in other military intelligence budgets.

Support the needs of a Counterproliferation Joint Interagency Task Force, the National Security Council, and other relevant consumers as the Intelligence Community's leader for interdiction-related issues. Counterproliferation interdiction, in a variety of forms, will remain an important part of combating the spread of nuclear, biological, and chemical weapons. The NCPC would play a vital intelligence support role both in helping to formulate U.S. interdiction strategies and in assisting in individual interdiction operations. The NCPC would also support strategic planning for interdiction efforts pursued by other government entities, including the Departments of Defense, State, Homeland Security, Commerce, and Treasury. Developing plans for and executing interdiction operations using the full capabilities of interagency, private sector, and international partners is a role appropriately played by a new Counterproliferation Joint Interagency Task Force, which we propose in Chapter Thirteen (Proliferation).

As noted above, we do not believe that, in addition to these important responsibilities, the NCPC should also be the focal point for strategic *policy* planning on countering nuclear, biological, and chemical proliferation. The Intelligence Community will inevitably be a major force in any interagency strategic planning process, but we believe it is inadvisable to "double-hat" another intelligence component with what is fundamentally a policy role, or to bifurcate the command structure overseeing it.[18]

Nevertheless, it is self-evident that *someone* should be performing strategic interagency planning on counterproliferation issues. As we will discuss in detail in Chapter Thirteen (Proliferation), the task of collecting intelligence on biological weapons and other proliferation threats is notoriously difficult; and we cannot reasonably expect intelligence alone will keep us safe. A successful counterproliferation effort will require a coordinated effort across the entire U.S. government, from the Intelligence Community to the Department of Defense to the Department of Commerce to the other agencies involved in this important work. In our more comprehensive later treatment of the counterproliferation challenge, we offer several recommendations on how to build

such a sustained interagency coordination process, including the creation of a joint task force for counterproliferation.

POTENTIAL PITFALLS ON THE PATH TO INTEGRATION

Our recommendations to this point have involved management strategies and organizational structures that could support the DNI's effort to forge an integrated Intelligence Community. In this section, we briefly identify two formidable challenges that may stand in the way of this objective. They both involve potentially problematic *relationships* for the Intelligence Community's leadership: namely, with the FBI and the Department of Defense.

Working with the FBI: Integrating Intelligence at Home and Abroad

Former Director of Central Intelligence James Woolsey told us that one of the most critical jobs of the new DNI will be to fuse the domestic and foreign intelligence enterprises.[19] This objective can only be achieved if the capabilities of agencies with intelligence responsibilities in the United States, like the FBI, are both strengthened and integrated with the efforts of other intelligence agencies. The FBI has made some significant strides in creating an effective intelligence capability, and we make substantial recommendations in Chapter Ten (Intelligence at Home) that we believe would further strengthen those capabilities.

There may, however, be speed bumps ahead for the DNI in ensuring that the FBI's intelligence resources are managed in the same manner as those within other Intelligence Community agencies. As we explain in detail in Chapter Ten (Intelligence at Home), the intelligence reform legislation is ambiguous in the extent to which it brings the FBI's analytical and operational assets into the Intelligence Community and under the DNI's leadership. We advise that this ambiguity be quickly resolved and suggest ways of making the DNI's authority over the FBI comparable to that of other intelligence agencies such as NSA and NGA—subject to, of course, the ongoing involvement of the Attorney General in ensuring the Bureau's compliance with laws designed to protect privacy and civil liberties.

Working with the Defense Department: Coordinating the National Intelligence Program with the Secretary of Defense

The most controversial sections of the intelligence reform act were those relating to the relationship between the DNI and the Secretary of Defense. This is not at all surprising, given the vital importance of effective intelligence support to military operations and the fact that many of the largest components of the Intelligence Community reside in the Department of Defense. These realities create an inherent challenge for any DNI seeking to bring order and coherent management to the Intelligence Community.

Recent events have highlighted the magnitude of this challenge. Over the past few months the Department of Defense has taken several steps to bolster its own internal intelligence capabilities. These have included initiatives to remodel defense intelligence that may enable Combatant Commanders to task and control national collection assets directly;[20] establishing the U.S. Strategic Command (STRATCOM) as the Global Intelligence, Surveillance, and Reconnaissance (ISR) manager for the Defense Department;[21] assigning the DIA as the key intelligence organization to support STRATCOM's ISR mission;[22] and building up the Defense Department's human intelligence capabilities to make the Defense Department less reliant on the CIA's espionage operations.[23]

We believe that several of these Defense Department initiatives are good ones, and should be supported. However, in all instances, we think these efforts need to be closely coordinated with the DNI—and in some cases we believe steps should be taken to ensure that the Defense Department's intelligence efforts do not undermine the new DNI's ability to manage the Intelligence Community. We identify four important issues pertaining to this relationship here: the need to balance support to military operations with other intelligence requirements; the importance of ensuring that the DNI maintains collection authority over national intelligence collection assets; the need to manage Intelligence Community agencies that reside in the Department of Defense; and the importance of coordinating Defense Department and CIA human intelligence operations.

Balancing support to military operations with other intelligence needs. Balancing the high priority, and often competing, demands on the U.S. Intelligence Community resources will be a significant challenge. The DNI will

need to develop processes for serving the military's requirements while preserving the ability to fulfill other national needs. Toward this end, we recommend the creation of a high level position within the Office of the DNI dedicated to military support. This individual would function as the principal military intelligence advisor to the DNI, serve as the Mission Manager for military support issues, and advise the DNI on issues of Defense Department-Intelligence Community coordination.

Ensuring that the DNI maintains authority over the tasking of national intelligence collection assets. If the Director of National Intelligence is to have any ability to build an integrated Intelligence Community, the DNI must be able effectively to manage national intelligence collection capabilities. To achieve this goal, we believe the Defense Department's requirements for national collection assets should be funneled through, not around, the DNI's integrated collection enterprise, outlined in Chapter Seven (Collection). In this process, the Defense Department's requirements for national intelligence collection in support of military operations will be represented by the DNI's principal military advisor. This individual will work closely with STRATCOM and the Combatant Commanders to ensure their needs for national intelligence support are met, and will lead the Target Development Board responsible for creating integrated collection strategies in response to U.S. military requirements. This process maintains the DNI's authority to manage national intelligence collection assets and increases the DNI's ability to effectively meet both the military's requirements and other national intelligence needs.

Developing clear procedures for the management of Defense Department agencies within the Intelligence Community. Many of the Intelligence Community's largest agencies reside within the Department of Defense. The new intelligence legislation's push towards unified intelligence management will further complicate the lives of the heads of these agencies, who will be uncertain whether they should answer to the Secretary of Defense or to the DNI. While some ambiguity is inevitable, there are certain steps that the DNI and the Secretary of Defense could take to add clarity in this area, including developing a joint charter that specifies each agency's reporting chain and operating authorities, and combining and coordinating management evaluations and audits to avoid needless and unproductive duplication of management oversight activities.

It is also critical that the DNI and the Secretary of Defense establish effective and coordinated protocols for exercising their acquisition authorities. As we have noted, the new legislation requires the DNI to share Milestone Decision Authority with the Secretary of Defense on all "Department of Defense programs" in the national intelligence budget. This important provision is also among the statute's more ambiguous ones, as the term "Department of Defense program" is undefined. As the success of these shared acquisition authorities is crucial to the fielding of future capabilities, we believe that the President should require the Secretary of Defense and the DNI to submit, within 90 days of the DNI's confirmation, their procedures for exercising shared Milestone Decision Authority, and a list of those acquisition programs they deem to be "Defense Department programs" under the legislation.

Coordinating Special Operations Command and CIA activities. The war on terrorism, and U.S. Special Operations Command's expanded role as the Defense Department's operational lead, have dramatically increased military intelligence interactions around the world. While the Defense Department has an organic human intelligence capability, the Department must closely coordinate its operations with the DNI to ensure deconfliction of operations and unity of purpose. We offer recommendations to address these coordination issues in our detailed discussion of human intelligence reform needs (Chapter 7, Collection). Here we recommend that the DNI and the Secretary of Defense, as part of their obligation to report to Congress within 180 days on joint procedures for operational coordination between the Defense Department and CIA,[24] address this specific issue of deconfliction with U.S. Special Operations Command.

Another Potential Pitfall: Legal Myths in the Intelligence Community

Throughout our work we came across Intelligence Community leaders, operators, and analysts who claimed that they couldn't do their jobs because of a "legal issue." These "legal issues" arose in a variety of contexts, ranging from the Intelligence Community's dealings with U.S. persons to the legality of certain covert actions. And although there are, of course, very real (and necessary) legal restrictions on the Intelligence Community, quite often the cited legal impediments ended up being either myths that overcautious lawyers had never debunked or policy choices swathed in pseudo-legal justifications. Needless to say, such confusion about what the law actually requires can seriously hinder the Intelligence Community's ability to be proactive and innovative. Moreover, over time, it can breed uncertainty about *real* legal prohibitions.

We believe this problem is the result of several factors, but for present purposes we note two. First, in the past there has not been a sizable legal staff that focused on Community issues. As a result, many Community problems were addressed through *ad hoc*, interagency task forces that tended to gravitate toward lowest common denominator solutions that were based on consensus and allowed action to be stalled by the doubts of the most cautious legal shop. Second, many rules and regulations governing the Intelligence Community have existed for decades with little thought given to the legal basis for the rules, or whether circumstances have changed the rules' applicability. Under such circumstances, it is unsurprising that legal "myths" have evolved.

The recent creation of a DNI General Counsel's office will increase the probability that Community legal issues are addressed more seriously. But the existence of the office alone does not guarantee an ongoing and systematic examination of the rules and regulations that govern the Intelligence Community. We therefore recommend that the DNI General Counsel establish an internal office consisting of a small group of lawyers expressly charged with taking a forward-leaning look at legal issues that affect the Intelligence Community as a whole. By creating such an office, the DNI will help ensure that the Intelligence Community is fully able to confront the many real—and imaginary—legal issues that will arise.

SUSTAINED OVERSIGHT FROM THE OUTSIDE AND IMPROVED SELF-EXAMINATION FROM WITHIN: MAKING SURE REFORM HAPPENS

Many—perhaps most—of the recommendations contained in this report have been made before. That we find ourselves proposing several sensible changes that former Secretary of Defense and Director of Central Intelligence James Schlesinger endorsed in 1971 suggests to us either that the Intelligence Community is inherently resistant to outside recommendations, or that it does not have the institutional capacity to implement them.[25] In either case, we are left with the distinct impression that meaningful intelligence reform proposals are only likely to become reality if the Intelligence Community receives sustained, senior level attention from knowledgeable outside observers. Today the Community receives only episodic oversight from the President's Foreign Intelligence Advisory Board (PFIAB), Congress, and a thinly-stretched National Security Council. We recommend several changes to improve this state of affairs.

Recommendation 7

We recommend that the Executive Branch improve its mechanisms for watching over the Intelligence Community in order to ensure that intelligence reform does not falter. To this end, we suggest that the Joint Intelligence Community Council serve as a standing Intelligence Community "customer council" and that a strengthened President's Foreign Intelligence Advisory Board assume a more vigorous role in keeping watch over the progress of reform in the Community.

We recommend that the Joint Intelligence Community Council (JICC) serve as a "customer council" for the Intelligence Community. The JICC, which was created by the recent legislation, consists of the heads of each department that has a component in the Intelligence Community. Chaired by the DNI, the JICC will include the Secretaries of State, Treasury, Defense, Energy, and Homeland Security, the Attorney General, and other officers designated by the President.[26] Although not a perfectly representative group of consumers, the JICC should provide the DNI with valuable feedback on intelligence products.[27] We do not think, however, that the JICC is the appropriate body to perform more sustained oversight of the Intelligence Community. Since the DNI chairs the JICC, and the members of the JICC

are heads of departments containing intelligence components, the body would have a "conflict of interest" that would impair its ability to play an independent oversight role.

We recommend that the President's Foreign Intelligence Advisory Board assume a more vigorous role with respect to the Intelligence Community. The PFIAB as it is currently constituted, however, is insufficiently equipped to accomplish this task. In addition to the seasoned national security policy experts now on the Board, a reinvigorated PFIAB would need more technical specialists able to assess Intelligence Community performance, as well as a larger staff to support the review and investigation tasks inherent in meaningful oversight. Such a PFIAB is not impossible to conceive, for it has existed in the past—as it should in the future.

Recommendation 8

We recommend that the President suggest that Congress take steps to improve its structure for intelligence oversight.

As a commission established by the President, we tread onto the terrain of congressional reform with some trepidation. The new intelligence legislation, however, contains a provision requiring the delivery of our report to Congress. As a result, we believe that it would not be inappropriate for us to make suggestions for reform in this area that the President could, in turn, recommend that the Congress implement.

The 9/11 Commission concluded in its final report that the Congressional intelligence committees "lack the power, influence, and sustained capability" necessary to fulfill their critical oversight responsibilities.[28] The 9/11 Commission offered two alternatives for overhauling the intelligence committees: (1) creating a bicameral committee, modeled on the Joint Atomic Energy Committee; or (2) combining intelligence authorization and appropriation authorities into a single committee in each chamber.[29] The House and Senate have not adopted either of these options. While we echo the 9/11 Commission's support for these proposals, we also recommend a number of more modest suggestions for improving Congressional oversight of intelligence.

Limit the activities of new intelligence oversight subcommittees to strategic oversight. Both the House and the Senate intelligence committees have indicated their intention to establish oversight subcommittees.[30] But these subcommittees will not improve intelligence if they simply demand additional testimony from top intelligence officials on the crisis or scandal of the day. We suggest that, if created, the oversight subcommittees limit their activities to "strategic oversight," meaning they would set an agenda at the start of the year or session of Congress, based on top priorities such as information sharing, and stick to that agenda.

Adjust term limits. The Senate has voted to remove term limits for the Senate Select Committee on Intelligence.[31] While the House may consider this too large a step, it could consider alternatives that would ensure the survival of institutional memory while also bringing in "new blood" and providing more members with exposure to intelligence issues. For example, the House could lengthen or even eliminate the term limits for some of the committee slots rather than for all of the slots. We suggest making the House leadership's authority to waive term limits explicit in the rules, and specifying that some positions on the intelligence committee would be free of term limits.

Reduce the Intelligence Community's reliance upon supplemental funding. There were good reasons for supplemental funding requests following the September 11 attacks. But for fiscal year 2005, nearly two-thirds of the key operational needs for counterterrorism were not included in the President's budget, and instead were put in a supplemental budget request later in the year.[32] This reduces the Intelligence Community's ability to plan operations and build programs. Instead of continuing to rely on large supplemental appropriations, we recommend that Congress and the President develop annual budgets that include the Intelligence Community's needs for the entire year and better allow planning for future years.

Adjust budget jurisdiction. Currently, the House and Senate oversight committees have different jurisdictions over the various components of the intelligence budget. Both committees have jurisdiction over the National Intelligence Program (NIP). The House intelligence committee also shares jurisdiction with the Armed Services Committee over the Joint Military Intelligence Program (JMIP) and Tactical Intelligence and Related Activities (TIARA) budgets. The Senate intelligence committee has no jurisdiction over JMIP or TIARA, although it provides advice to the Armed Services

Committee on both budgets. This complicates conferences on the intelligence authorization bill and reduces intelligence committee input into the JMIP and TIARA budgets. We recommend broadening the Senate intelligence committee's jurisdiction to include JMIP and TIARA in order to integrate intelligence oversight from the tactical through to the national level.

Allocate the intelligence budget by mission, rather than only by program or activity. The DNI can also take steps to streamline and professionalize the intelligence oversight process. One impediment to Congressional evaluation of the intelligence budget is the way the budget is presented. Because line items track specific technologies or programs rather than mission areas, it is nearly impossible for Congress—or the Executive Branch—to evaluate how much money is being spent on priority targets such as terrorism or proliferation. We recommend that the DNI restructure the budget by mission areas, thus permitting greater transparency throughout the budget cycle. This mission-centered budget would permit the individual Community elements to track their expenditures by mission throughout the year, affording the DNI greater flexibility in managing the Community, and the Executive Branch and Congress an increased ability to provide effective oversight.

Deter unauthorized disclosures. More substantive Congressional oversight must be accompanied by a strengthened commitment to protect sensitive information from unauthorized disclosure. The Congress has rules to protect sensitive information and a process for investigating and penalizing those who violate those rules.[33] In some instances, however, unauthorized disclosures have either been ignored or treated lightly. The Senate and House leadership should place greater emphasis on ensuring that all members understand the need to carefully protect sensitive information and the penalties for unauthorized disclosures. For example, the leadership could make clear that all unauthorized disclosures of classified information will be referred to the ethics committees. Furthermore, both Senate and House members who are read into sensitive compartments should follow the same nondisclosure procedures applicable to the Executive Branch.[34]

Improve committee mechanisms to encourage bipartisanship. Partisan politics should never be allowed to threaten national security. To foster bipartisanship, we recommend that the House intelligence committee consider adopting provisions similar to those in the Senate, such as designating the ranking member as the Vice Chairman of the committee, requiring that the majority

maintain no more than a one-member advantage in membership, and ensuring that the rules provide the majority and minority leaders with equal access to committee information. The committees could also take concrete steps to reinforce close, cooperative relationships among the entire staff. For example, regular joint staff meetings could be encouraged or even required. Perhaps most importantly, the staff should consist of national security professionals focused on the objectives and priorities of the committee.

Encourage more informal discussions and collaboration between the Intelligence Community and its congressional overseers. The Intelligence Community typically interacts with Congress in formal ways, through briefings to the intelligence committees and formal testimony. However, there also have been occasional "off sites" at which senior lawmakers and Intelligence Community leaders have met in a more informal and less adversarial setting. Both sides have stressed the value of these informal sessions, both in fostering cordial cross-branch relationships and in increasing bipartisanship among lawmakers. We encourage the expanded use of these and other informal collaborative efforts.

Consider an intelligence appropriations subcommittee. While the intelligence authorizing committees are well-staffed and completely focused on the Intelligence Community, the intelligence appropriations are simply a small part of the Defense and other appropriators' jurisdiction, so staffing and attention to intelligence issues are in short supply on the appropriations committees. The resulting mismatch reduces oversight and coordination of policy within Congress. While we recognize the difficulties, we suggest that serious consideration be given to the establishment of an appropriations subcommittee focused exclusively on the intelligence budget.

Look for ways to reduce the cost of oversight in the Intelligence Community. With so many congressional committees with jurisdiction over aspects of foreign and domestic intelligence, the oversight process—between staff requests, formal testimony, congressionally directed actions, and budget reviews—imposes great demands on the resources of the Intelligence Community. Intelligence Community professionals collectively appear before Congress in briefings or hearings over a thousand times a year, and also respond to hundreds of formal written requests from Congress annually[35] —and the latter number will only increase in light of the recent intelligence reform legislation, which itself added 27 one-time and 16 annual reports to the DNI's annual congressional

reporting requirements. While we recognize that congressional oversight inherently has costs, we encourage the Congress to look for ways to streamline their interactions with the Intelligence Community.

Recommendation 9

The Intelligence Community should improve its internal processes for self-examination, including increasing the use of formal "lessons learned" studies.

As important as executive and legislative oversight is, they will never be a substitute for an Intelligence Community that takes self-evaluation seriously. But the Intelligence Community has done far too little to institutionalize "lessons learned" studies and other after-action evaluations that are commonplace in the Department of Defense and other government agencies. Of course, when human resources are stretched thin, the idea of devoting good personnel to examine the past often seems a luxury that intelligence agencies cannot afford.

Understandable as it is, this view must be resisted. Over the long run, an organization with sound "lessons learned" processes will be more efficient and productive—even if those processes seem to be distracting good people and resources from the imperatives of the moment. We recommend that the DNI develop institutionalized processes for performing "lessons learned" studies and for reviewing the Intelligence Community's own capabilities, rather than waiting for commissions like ours to do the job. In a separate chapter we offer a recommendation in this regard that is specific to analysis, (see Analysis, Chapter 8)—but this is a problem that affects all areas of intelligence. While we think it advisable that organizations devoted to self-evaluation exist in all major intelligence agencies, the DNI must drive an independent "lessons learned" process as well—for it is the DNI who will have insight into shortcomings and failures that cut across the intelligence process. We also note that whatever entities at the DNI or agency level assume these after-action responsibilities—be they agency inspectors general or other offices—they should not conduct these reviews to justify disciplinary or other personnel action, but rather to identify shortcomings and successes and to propose improvements to aspects of the intelligence process.

CONCLUSION

The creation of an integrated Intelligence Community will not happen merely by improving activities within different agencies, and it will most certainly not happen spontaneously. It will take assertive leadership by the new DNI, vigorous support from senior policymakers and Congress, and sustained oversight from outside the Intelligence Community. Provided all that, and substantial time, a Community that has resisted management reform—and often management of any sort—can emerge better configured to deal with the pressing challenges of the new century.

ADDENDUM: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

In our discussion of management issues the DNI will confront, we have tried to eschew the "boxology" that often dominates discussions of government reform. While it is obviously important to consider what staff functions will be performed in the Office of the DNI, precise organizational questions about the structure of the office—such as, for instance, the number of deputies the DNI should have and their responsibilities—are questions to which there is no "right answer." Nonetheless, when considering the tasks that will need to be performed in the office of the DNI, we necessarily had to consider how the office might be organized to perform these functions. We offer here the result of these considerations, but we emphasize that the model we propose is a notional one that we offer only to facilitate further discussion.

The new legislation creates a number of positions in the Office of the Director of National Intelligence. The statute creates a Senate-confirmed principal deputy to the DNI, and empowers the DNI to appoint up to four deputy directors. In addition, the statute also states that the Office of the DNI shall contain a General Counsel, a Director of Science and Technology, a National Counterintelligence Executive, a Civil Liberties Protection Officer, and the National Intelligence Council. Finally, the legislation provides that the Office of the DNI *may* include "[s]uch other offices and officials as may be established by law or the Director may establish or designate in the office," including "national intelligence centers." Of these various mandated and discretionary offices, only one—the Civil Liberties Protection Officer—is required by the act to "report directly to" the DNI;[36] in our view, the remainder can therefore report to the Director through one of the four Deputy DNIs (DDNI) permitted under the legislation.

The notional model described below—and depicted on the wiring chart at the end of this chapter—is structured around four Deputy Directors: a Deputy Director for Integrated Intelligence Strategies; a Deputy Director for Collection; a Deputy Director for Plans, Programs, Budgets, and Evaluation; and the Chief Information Management Officer. We also suggest the creation of two additional positions: an Assistant DNI for Support to Military Operations, and an Assistant DNI for Human Resources. The section that follows briefly describes the responsibilities of each of these subordinate offices.

Deputy DNI for Integrated Intelligence Strategies

We have stressed the need for ensuring that the Intelligence Community's management structure be focused on missions, and propose the creation of Mission Managers to ensure that intelligence collection is driven by the needs of analysts, policymakers, and other intelligence "customers." In our proposed organizational structure for the Office of the DNI, Mission Managers would be housed in the office of a Deputy DNI for "Integrated Intelligence Strategies." This office would also perform the following functions (often through the Mission Managers):

Mission Manager coordination, support, and oversight. The Deputy Director for Integrated Intelligence Strategies would advise the DNI on the intelligence subjects that require Mission Managers, and develop processes for the periodic review of those subjects to ensure that new priority intelligence topics are not missed. He or she would also oversee the Mission Managers and resolve disputes among them in those (we expect rare) situations where they disagree among each other over the prioritization of intelligence requirements.

Customer support. Mission managers will be the primary interface for customer support on their substantive topics, but the DDNI for Integrated Intelligence Strategies would establish procedures to improve customer support across the Intelligence Community and assess new ways to improve the ways in which policymakers and other users receive intelligence support.

Analytical oversight. The office of the Deputy Director for Integrated Intelligence Strategies would be responsible for overseeing the analytical community (often through Mission Managers), reaching out to subject-matter experts outside of the Intelligence Community (and developing procedures and processes for analysts throughout the Community to do the same), and encouraging the development and mainstreaming of new analytical tools.

Current intelligence support to the DNI. In fulfilling his role as principal intelligence advisor to the President, the DNI will require a support staff. This staff would be housed in the Office of the Deputy Director for Integrated Intelligence Strategies, who would serve as the DNI's principal intelligence expert.

Deputy DNI for Collection

Both in this chapter and in our later chapter devoted to Collection (Chapter 7), we emphasize the need for Community-level leadership of vital collection functions that today are not centrally managed. We would create a Deputy DNI for Collection to perform this role. One of this official's most important functions would be to oversee the customer-driven collection requirements process managed by the Mission Managers and their Target Development Boards. The Mission Managers should provide the needed analytic input directly to collection agencies, but there must be a mechanism to ensure that intelligence collectors are responding to those requirements. The Deputy DNI for Collection would also perform the following functions:

Strategic oversight of collection. The Office of the Deputy Director for Collection would monitor the performance of collection agencies in responding to all customer needs, including, most importantly, the requirements developed by Mission Managers and Target Development Boards and those that ensure that U.S. military commanders and forces are also appropriately supported. It would also oversee the development of the "integrated collection enterprise" we recommend in Chapter Seven (Collection).

Development of new collection sources and methods. When collection requirements cannot be met because of insufficient capabilities, this office would spur the development of new sources and methods to overcome the capability gap. This office would play an especially important role in sponsoring those new capabilities whose interoperability across collection agencies is critical to Community collaboration. Efforts to identify new capabilities will include outreach to U.S. government laboratories, industry, and academia, as appropriate.

Strategic investment for Community collection. When collection requirements cannot be met because of insufficient capability, and new technologies and systems are required, the Deputy DNI for Collection would advocate innovative science and technology for collection applications, and would ensure such capability requirements are addressed in the development of the National Intelligence Program (NIP) budget, and in the DNI's inputs to the Joint Military Intelligence Program (JMIP) and Tactical Intelligence and Related Activities (TIARA) budgets.

Deputy DNI for Plans, Programs, Budgets, and Evaluation

As we have noted, the DNI's primary leverage will come not through "line" control of Intelligence Community agencies, but rather from his budgetary authorities. We would establish a Deputy DNI for Plans, Programs, Budgets, and Evaluation (PPBE) to ensure that this authority is exercised promptly and completely. The Deputy DNI for PPBE's most significant functional responsibilities would include:

Plans and policy. The DNI is responsible for developing and presenting the NIP budget and for participating in the development of the JMIP and TIARA budgets.[37] To develop a rational investment balance to meet customer needs, the DNI will have to evaluate the capabilities of the Community, develop options for resource allocations, and propose specific programs submitted for inclusion in the NIP.

Comptroller. As a financial manager, the DNI is responsible for executing the NIP and reprogramming funds within limits established in the new legislation.[38] In performing these duties, the DNI will require a staff element to fill these comptroller functions.

Acquisition. The reform legislation makes the DNI the Milestone Decision Authority for major acquisition systems funded in whole within the NIP and assigns the DNI responsibility to procure information technology systems for the Intelligence Community. Through the Deputy DNI for PPBE, the DNI would set acquisition policy, provide acquisition oversight, and act as program manager for all Community systems whose interoperability is essential to Community effectiveness. As we have noted, for the major systems over which the DNI and the Secretary of Defense share acquisition authority, joint procedures must be established with the Defense Department.

Program evaluation. The Deputy DNI for PPBE would be responsible for analyzing and evaluating plans, programs, and budgets in relation to Community objectives and requirements, and for ensuring that costs of Community programs are presented accurately and completely.

Chief Information Management Officer

One of our major information sharing recommendations is that the DNI appoint a chief information management officer (CIMO) who would manage

the information sharing environment for the Intelligence Community. Given the importance of the development of such an environment, we would make the CIMO one of the DNI's Deputies. We detail the CIMO's responsibilities in our chapter on Information Sharing (Chapter 9), but we emphasize here that this individual would be responsible both for information *sharing* and information *security* across the Intelligence Community. As the attached organizational chart suggests, we would have the CIMO supported by three separate component offices dedicated to information sharing, information security and protection of sources and methods, and risk management.

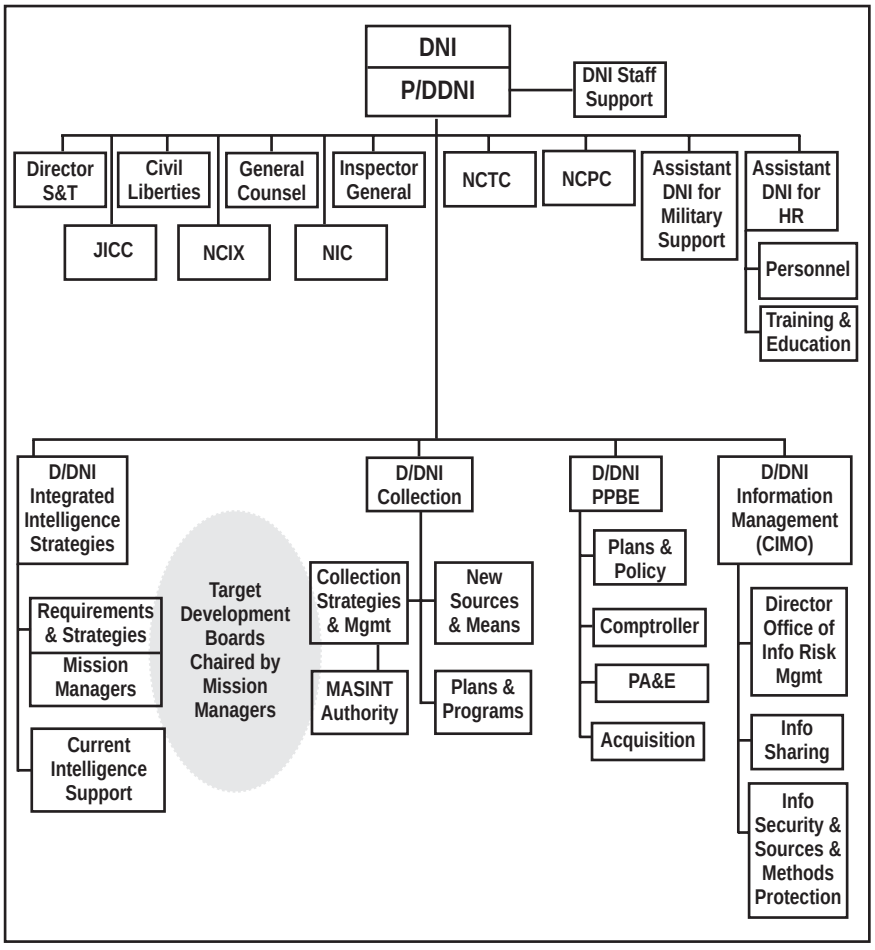
Assistant DNI for Support to Military Operations

The Director of Central Intelligence (DCI) currently has an Associate DCI for Military Support—a position created in the wake of Operation Desert Storm to provide a high level military representative on the DCI's staff whose mission was to improve the Intelligence Community's support to military operations. Incumbents in this position have been three-star officers, normally with a combat-arms background. As we have noted in our management discussion, in the wake of the intelligence reform legislation the relationship between the DNI and the Secretary of Defense will assume great significance. Accordingly, we would suggest that a similar—and strengthened—military support position be created in the Office of the DNI who would act as principal advisor to the DNI on military support issues, serve as Mission Manager for intelligence support to military operations, and assist the DNI in developing joint strategies and coordination procedures between the DNI and the Secretary of Defense.

Assistant DNI for Human Resources

The intelligence legislation provides the DNI with substantial personnel authorities, and we recommend earlier in this chapter that a DNI-level Human Resources Authority be established to develop and implement appropriate personnel policies and procedures for the Intelligence Community. We would propose that an Assistant DNI for Human Resources oversee this Human Resources Authority, and oversee the substantial changes in recruiting, training, and personnel policy that we believe are necessary. The Assistant DNI for Human Resources would also oversee the National Intelligence University that we recommend in this chapter.

A Notional Organization of the Office of the Director of National Intelligence



ENDNOTES

[1] While the 15 organizations within the Intelligence Community are not all technically "agencies"—some are instead designated as "bureaus" or "offices" within executive departments or military services—we at times refer to them collectively as "agencies," for the sake of simplicity and convenience. For a more detailed description of the components of the Intelligence Community, please see our Overview of the Intelligence Community at Appendix D of this Report.

[2] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-458 (hereinafter "IRTPA").

[3] Interview with senior Department of Defense official (Oct. 4, 2004).

[4] The DNI is to "determine" and guide the development of the NIP and the budgets for the Community's component agencies. IRTPA at § 1011. Moreover, in contrast to the DCI, whose formal participation in the budget process ended when the annual budget was prepared, the DNI both directs the allocation of National Intelligence Program appropriations and can "ensure the effective execution" of the annual intelligence budget. Perhaps most importantly, while the DCI could not transfer national intelligence program funds within the budget of an intelligence agency without approval of the agency's department head, the DNI can transfer up to $150 million annually (or 5 percent of a given intelligence agency's budget) without approval. *Id*.

[5] The overall budget for intelligence is divided into three separate programs: the National Intelligence Program; the Joint Military Intelligence Program (JMIP); and the programs for Tactical Intelligence and Related Activities (TIARA). The Secretary of Defense has primary authority to develop the annual JMIP and TIARA budgets, although the new legislation states that the DNI shall "participate" in the development of these processes. *Id*.

[6] The DNI has exclusive Milestone Decision Authority only for major system intelligence acquisition programs that are not in the Department of Defense. The DNI must share Milestone Decision Authority with the Secretary of Defense for systems funded by the NIP that are within the Defense Department, and lacks even joint Milestone Decision Authority over major system intelligence programs that rely in whole or in part on the Defense Department's joint military or tactical intelligence program funds. *Id*.

[7] *Id*.

[8] *Id*.

[9] Some have suggested—drawing on a loose analogy to the military's use of "joint commands"—that the best way to accomplish this task is to divide the universe of intelligence into "national intelligence centers." As we discuss later in this chapter, while we believe that centers can and should be used in certain circumstances, we are less enthusiastic about the idea of using centers as a generally applicable organizational model for tackling intelligence problems, and believe the Mission Manager concept to be superior for this purpose.

[10] IRTPA at § 1011.

[11] *See, e.g.*, James R. Locher, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon* (2002); Commission on the Roles and Capabilities of the United States Intelligence Community (i.e., Aspin-Brown Commission), *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996).

[12] DCI Community Management Staff, *NFIP—Funds by Selected Topic: Education and Training* (Dec. 7, 2004) (prepared at the Commission's request).

[13] Interview with senior CIA official (Dec. 9, 2004).

[14] IRTPA at § 1021 (on the NCTC) and § 1022 (on the NCPC).

[15] *Id*. at § 1022.

[16] While we believe that chemical weapons are not a threat of the same order as nuclear and biological weapons, there are sufficient areas of overlap between the processes for collecting intelligence on these three categories of weapons to justify the inclusion of chemical weapons in the NCPC's mission. It is critical, however, that resources at the NCPC be allocated among these weapons types in a manner that is proportionate to the threat.

[17] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004) at p. 410 (hereinafter "9/11 Commission Report").

[18] We recognize that the Intelligence Community implements policy when it executes covert action, but this is done (we think appropriately) with very strict oversight and in relatively limited circumstances.

[19] Interview with R. James Woolsey, former Director of Central Intelligence (Aug. 24, 2004).

[20] Interview with senior Defense Department official (Feb. 3, 2005).

[21] Interview with senior Defense Department official (Jan. 13, 2005).

[22] *Id*.

[23] Interview with senior Defense Department official (Feb. 3, 2005).

[24] IRTPA at § 1013.

[25] James Schlesinger, A *Review of the Intelligence Community* (Mar. 10, 1971).

[26] IRTPA at § 1031.

[27] The JICC as currently composed does not include a representative from the Executive Office of the President, or other parts of the Executive Branch that do not include elements of the Intelligence Community. The President could easily solve the problem of no White House representation by making the Special Assistant to the President for National Security Affairs a member of the Council.

[28] 9/11 Commission Report at p. 420.

[29] *Id*.

[30] The U.S. House of Representatives has created a Subcommittee on Oversight for the 109th Congress. The Senate has to date not created one although there is ongoing discussion of the issue.

[31] Senate Resolution 445, 108th Congress, 2nd Session (Oct. 9, 2004).

[32] Interview with DCI Community Management Staff official (Feb. 23, 2005); CIA, *Response to Document Request # 74, Question 2*.

[33] *Rules of the Select Committee on Intelligence, Congressional Record* (Feb. 25, 2003) at pp. S2689-S2694.

[34] HPSCI staff members are required by HPSCI Rules 12(b)(2) to sign a Non-Disclosure Agreement. Both Members and staff are bound by the House Rules regarding non-disclosure of classified material. Senate Rule 10.5 also contains a requirement of a Non-Disclosure Agreement for SSCI staffers.

[35] Office of the DCI, Submission to Commission (March 2005).

[36] IRTPA at § 1011.

[37] *Id*.

[38] *Id*.

CHAPTER SEVEN
COLLECTION

Summary & Recommendations

The collection of information is the foundation for everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information—as our Iraq study demonstrated—turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most.

This chapter sets forth our recommendations for improving the collection capabilities of our Intelligence Community so that it is better equipped to confront today's diffuse, elusive, and ever-changing intelligence challenges. These recommendations fall into two categories: those focused on improving the performance of particular collection agencies, and those aimed at integrating the management of collection across the Intelligence Community. Among other suggestions, we recommend that the DNI:

- Create an "integrated collection enterprise"—that is, a management structure that ensures that the Intelligence Community's decentralized collection capabilities are developed in a manner that is consistent with long-term strategic intelligence priorities, and are deployed in a coordinated way against today's intelligence targets;
- Encourage the development of new and innovative human intelligence collection techniques, and empower the CIA to coordinate the full spectrum of human intelligence activities performed in the Intelligence Community; and
- Establish an Open Source Directorate in the CIA responsible for collecting and storing open source information, and developing or incorporating commercial tools to assist users in data searches—including those in foreign languages.

INTRODUCTION

The Intelligence Community exists, first and foremost, to collect information vital to the national security of the United States. This may seem self-evident, but it bears restating—for as our case studies demonstrate, there are simply too many gaps in our understanding of too many serious national security threats. Our Iraq case study found a near complete failure across all of the Intelligence Community's collection disciplines—from those who collect human intelligence, to the technical collection agencies that take satellite photographs and intercept communications—to gather valuable information on Saddam Hussein's weapons capabilities. And our broader review found that Iraq was not an isolated case. From Iran's pursuit of nuclear weapons to the inner workings of al-Qa'ida, the Intelligence Community frequently admitted to us that it lacks answers.

The collection challenges facing the Intelligence Community are certainly daunting. In addition to maintaining the ability to penetrate closed societies—a capability that proved essential to the conduct of foreign policy during the Cold War and that remains vital today with regard to states including China, North Korea, and Iran—the Community also faces the imperative of collecting against secretive transnational organizations that operate globally. At the same time, modern warfare requires that national intelligence collectors both support strategic planning needs and offer real-time assistance to military operations. In short, the Community is facing unprecedented demands to do it all, and to do it all very well.

It is clear that the old ways of doing business will not suffice to meet these challenges. For example, the "traditional" model for collecting human intelligence is ill-suited to confront some of today's most critical intelligence challenges. And traditional technical collection techniques have been degraded by the pace of change in telecommunications technology and by our adversaries' increasing awareness of our capabilities. It therefore came as no surprise to us when we found that many recent intelligence successes resulted from more innovative collection techniques. But as these innovation efforts are still episodic and far too rare, in this chapter we offer recommendations aimed at encouraging our intelligence agencies to develop new ways of collecting information—ranging from methods for conducting human intelligence, to finding technologies for exploiting the massive amount of "open source"

information now available on the Internet and in other publicly available sources.

But to focus only on developing new techniques would be to confront only half of the collection challenge. Of equal importance—and consistent with our call for greater integration throughout the Intelligence Community—we found that collectors too often operate independently. Our largely autonomous collection agencies have not been accountable to any central authority within the Intelligence Community for the investments they make or the quality of intelligence they collect. Moreover, because they do not coordinate their activities, opportunities for highly promising collaborative collection are often missed. Therefore, we also propose that the Intelligence Community's collection capabilities be managed as an "integrated collection enterprise"—that is, we need a collection process that is strategically managed and coordinated at every step, from investment in research and development, to the acquisition of technical systems, to the formulation and implementation of coordinated cross-agency strategies for deploying our collection resources.

Despite the difficulty and diversity of the challenges facing the Intelligence Community, the excuse "it's too hard" plainly will not suffice. We must reconfigure the Community's collection capabilities in ways that enable it to reduce uncertainty against key intelligence threats. This chapter offers our recommendations for accomplishing this objective.

THE TARGETING CHALLENGE

Our recommendations are designed to increase the Intelligence Community's ability to collect against today's targets as well as expected targets of the future. As a starting point, however, it is worth considering how our collection system got where it is today, and why the rapidly changing nature of many threats makes that system so inadequate.

The Cold War

Throughout the Cold War, the United States focused its collection efforts against monolithic Communist powers—the Soviet Union and China—and their proxy states. These targets had sizeable military and industrial complexes that our satellites could observe, and they had hierarchical institutions, predictable communications procedures, and reporting behavior that we could

selectively target for eavesdropping. As a result, although penetration took time and was far from perfect, on the whole the Intelligence Community gained an impressive understanding of our main adversaries.

During this period, a number of intelligence agencies—the National Security Agency, the National Reconnaissance Office, and others—developed around the various technologies and disciplines used to collect against these targets.[1] These agencies were largely independent entities capable of determining their own strategies with only general guidance from above. As a general matter, they engaged in limited collaborative collection, and each (unsurprisingly) tended to invest in the research and development of technologies for collecting on the traditional Cold War targets. They did not (nor, perhaps, could they) anticipate the very different threats that we face today.

Today's Targets

In contrast to the Cold War, today's collection environment is characterized by a wider spectrum of threats and targets. For example, non-state actors such as al-Qa'ida present a new type of asymmetric menace. They operate globally, blending into local society and using informal networks for support. Locating and tracking dispersed terrorists and guerrilla fighters hiding in an urban environment—rather than massed armored forces on a European battlefield—typifies the type of collection problems the Intelligence Community faces today.[2] Such dispersed targets can, and often do, communicate chiefly through methods that are difficult to detect and that some of our collection systems are poorly suited to penetrate. In sum, today's threats are quick, quiet, and hidden.

Of course, state actors like Russia, China, and North Korea also continue to require attention. But for several reasons, penetrating these targets has also become more difficult than ever before. For example, authorized and unauthorized disclosures of U.S. sources and methods have significantly impaired the effectiveness of our collection systems. Put simply, our adversaries have learned much about what we can see and hear, and have predictably taken steps to thwart our efforts.[3] In addition, the changing face of weapons technology now means that certain weapons types, particularly biological and chemical weapons, can be produced in a manner that is difficult or impossible to detect.[4] All of this implies that the Community's effectiveness will continue to decline in the coming years unless concerted change occurs.[5]

Addressing Today's Collection Demands

It's not just that targets have changed; demands for collection have also shifted. Most significantly, since the first Gulf War, U.S. military requirements for national intelligence have spiked.

In the not-too-distant future, the U.S. military hopes to achieve a common operating picture of the battlefield in real time using a diverse set of tactical, national, and commercial sensors and communication technologies. This force transformation will create new requirements for collection and necessitate new approaches to fusing and integrating data to enable real-time analysis. And although the military's vision is not yet a reality, current demands have already put a strain on finite collection capabilities.

As a result, military requirements on national collection systems (such as satellites) have already diminished our effectiveness with respect to other targets important to national decisionmakers. For example, a study of why the Intelligence Community failed to warn of the surprise nuclear tests in India in May 1998 found that limited collection on India test sites was explained, in part, by its low priority owing to competing military requirements.[6] More recently, we found that support to current military operations in Iraq diverted imagery collection resources that would otherwise have been available to obtain information on nuclear developments on other priority targets in the region.

Regrettably, the Intelligence Community does not currently have a systematic process for balancing these competing interests. Today, the Assistant DCI for Collection and the Under Secretary of Defense for Intelligence meet frequently to discuss collection issues, including the allocation of national intelligence systems to support the needs of the military. However, neither individual has the requisite authority or resources to routinely develop and direct the implementation of integrated target development strategies.[7] As a result, the Intelligence Community has tended not to use its available collection systems efficiently.

This inefficiency is merely illustrative of a larger problem—the absence of methods for prioritizing and coordinating our Intelligence Community's decentralized collection capabilities. No office or individual sets long-term research and development priorities, acquires necessary capabilities, and formulates and implements an integrated collection strategy from a Community-

wide perspective. Instead, each of these functions is run by a panoply of different intelligence collection organizations.

Our case study of Iraq found that such disaggregation sometimes undermined effective intelligence gathering. Other studies we conducted, including those involving Iran's nuclear program and North Korea, further concluded that the current collection system has limited ability to engage in long-term, coordinated planning on existing threats, let alone to anticipate surprises. As a result, intelligence collection appears to be consistently behind the curve in identifying change, and it is usually positioned to be reactive rather than proactive—when it needs to be both.

Many of these observations—and our associated recommendations—are not new. Several decades of studies of the Intelligence Community have identified the lack of a unified, coherent collection process as a major shortcoming of the Community.[8] These studies recognized that under the existing system, no one other than the President, who obviously lacks the time for such a detailed task, has the clear authority to direct all of the nation's collection assets. This absence of central authority has impeded the development and implementation of unified strategies that operate existing collection assets against "hard targets."[9] In today's threat environment, we cannot wait decades longer to remedy these problems.

CREATING AN "INTEGRATED COLLECTION ENTERPRISE"

Recommendation 1

The DNI should create a new management structure within the Office of the DNI that manages collection as an "integrated collection enterprise." Such an integrated approach should include coordinated target development, collection management, data management, strategic planning and investment, and the development of new collection techniques.

Intelligence collection is a massive endeavor. In order to collect effectively, the Intelligence Community must develop, buy, and operate collection systems, manage the data that the systems collect, and plan for the acquisition of future systems. It is this cradle-to-grave process that we refer to as the "col-

lection enterprise." As the following makes clear, the Mission Managers we proposed in our chapter on management will play an integral role in nearly every facet of this integrated structure. There are five key components to this enterprise:

Target development: The process of defining collection priorities, determining existing collection gaps, and developing integrated collection strategies to address those gaps;

Collection management: Ensuring the effective implementation of the integrated collection strategies across the collection disciplines;

Data management: Supervising the processing, exploitation, movement, and analysis of data that is collected through each of the different collection disciplines;

Strategic planning and investment: Evaluating different investment alternatives, considering budgetary tradeoffs, and establishing long-term acquisition strategies; and

Developing new collection techniques: Evaluating current collection methods, designing new methods (including new platforms for human intelligence), and establishing research and development programs to fill intelligence needs.

As we have already discussed, each of the five functions we identify is currently performed primarily within individual collection agencies. The goal of our recommendation is to create an integrated collection process that performs each of these functions from the perspective of the *entire* Intelligence Community, rather than individual agencies. This is not to say that there are no benefits to the current decentralized approach to intelligence collection. We recognize, for example, that each agency understands its own capabilities best and is, in many ways, able to optimize its own efforts.

Our recommendation therefore attempts to build on these strengths. The new integrated enterprise will draw on the technical expertise possessed by each collector, but will also demand that agencies work together to ensure that all forms of collection are used where they are most needed and effective. We also do not expect the new collection enterprise to displace existing

personal relationships between collectors and analysts that allow analysts to provide additional clarifications or tasking. We do expect, however, that the centralized process we propose would ensure that the resources of our collection agencies are marshaled in a more strategic, cost-effective, and coordinated way.

We consider each of the key components of this integrated enterprise in turn.

Integrated Target Development

Recommendation 2

Target Development Boards, which would be chaired by the Mission Managers, should develop collection requirements and strategies and evaluate collectors' responsiveness to these needs.

Current collection processes are unique to each collection discipline and are often supported by complex and opaque "requirements systems." This typically means that in order to ask a collection agency to gather intelligence on a particular issue, analysts must forward their intelligence needs to their organization's collection managers or to discipline-specific Community collection committees, which in turn send collection requirements to specific collection agencies. Some analysts may also submit informal, *ad hoc* requests to their working-level associates and counterparts in collection organizations. Each collection agency then works independently to satisfy the "customer"—meaning, in this case, the analyst.

This rather haphazard process is occasionally prodded or refined by the intervention of the Assistant Director of Central Intelligence for Collection and his National Intelligence Collection Board (NICB), whose members represent the collection agencies. The board members meet to discuss and review some high-priority intelligence issues and the efforts by individual collection agencies to fulfill the associated collection requirements. We believe that this process has shown itself to be inadequate to the collection challenges facing the Community today, and that a more integrated strategy—one that would consolidate information needs and collection capabilities in one forum—would be a dramatic leap forward. We recommend the establishment of standing Target Development Boards for this purpose.

In our chapter on management (Chapter 6), we recommend that the DNI establish several "Mission Managers" who would be responsible for managing both analysis and collection on a particular intelligence target. Each Mission Manager would chair a Target Development Board, which would precisely define and prioritize information needs for that Mission Manager's subject area, determine existing intelligence gaps, and develop collection strategies to address them. As this list of responsibilities suggests, the boards would comprise both analysts and collectors from all relevant agencies and the military. Board members would have full visibility into the range of collection capabilities (including, as needed, those that are especially sensitive). The boards, led by the Mission Manager, would develop collection strategies that would serve as the blueprint for the Community's collection efforts. The boards would also provide a forum for discussing the optimal way to conduct those efforts. Ultimately, Target Development Boards would assess whether collectors have fulfilled their information needs[10] —and if they determine that existing collection capabilities cannot fulfill these requirements, Mission Managers could recommend that research and development of particular new sources and technologies are needed.

We have purposely avoided addressing the question of comprehensively listing which issues should be served by Mission Managers. In our view, the new DNI will be best situated to evaluate what issues are most pressing and therefore require Mission Managers. That being said, we believe the DNI should develop clear processes for defining the scope of responsibility for new Mission Managers and for phasing out—or "sunsetting"—Mission Managers whose missions no longer warrant such attention. We think this last point is critical, for one of the advantages we see in Mission Managers, as opposed to more permanent centers, is the flexibility they offer the DNI to adjust to shifting priorities. Finally, the DNI might consider establishing a "Global Issues Mission Manager" to serve as a "catch-all" for any number of issues that require special attention yet do not require their own Mission Manager.

Strategic Management of Collection

Target Development Boards would send baseline requirements for their issue directly to collection agencies (*e.g.*, NSA, NGA, CIA). In addition, a consolidated, prioritized list of all the target board requirements—reflecting the priorities of the President, other key decisionmakers, and the military—would be

developed on a periodic basis to provide strategic guidance to collectors as to the nation's most important information needs and to ensure a balance is maintained between national intelligence collection support to military operations and other national priorities.

The part of the DNI's office responsible for managing national intelligence collection resources would work with the Mission Managers to ensure that their consolidated collection strategies are executed efficiently, and would resolve conflicting requirements. This part of the DNI's office would be best suited to strategically oversee the implementation of the integrated Target Development Board strategies by guaranteeing that collection agencies were in fact targeting the identified priorities and making sure that each collection system was targeting the intelligence gaps that it is best suited to address. This same entity could monitor overall developments within the collection organizations and would assist the Mission Managers by keeping them informed of collection activities and helping to evaluate the performance of collectors.

Introducing Mission Managers, Target Development Boards, and a strategic management element to the collection process would thus address several specific, serious flaws that were identified in our case studies by providing a permanent mechanism for identifying current and future intelligence gaps and pairing those gaps with the capabilities required to fill them, a forum for developing strategies that optimize resources by reducing redundancy and maximizing opportunities to use the various collection disciplines in tandem or complimentary fashion, and a formalized system for ironing out competing collection priorities across the Community.

Targeting in an Integrated Fashion

What might the target development and strategic management components of the integrated collection enterprise mean in practice? We anticipate that the basic process might work much as described in the following scenario if the DNI were to designate a Mission Manager for Country X:

Targeting in an Integrated Fashion (Continued)

We envision that the Country X Mission Manager, in conjunction with analysts and the Country X Target Development Board, will identify the most important subject matter areas relating to Country X's nuclear program. The Target Development Board will then study all available collection capabilities against the target and craft a strategy that matches those capabilities from across the Community to the intelligence "gaps" we have in our understanding of Country X's program. If collectors come up short in filling these "gaps," the Mission Manager may recommend more aggressive collection techniques involving higher risk strategies. Because it is a standing entity, the Target Development Board will be able to quickly revisit priorities in response to changing events, and adjust the collection strategy correspondingly.

Having developed a collection strategy, the Mission Manager then will forward collection requirements to various collection agencies—NSA, NRO, CIA, DIA, and others. A collection-focused office in the DNI's office (perhaps a Deputy DNI for Collection), assisted by the Mission Manager, will work to ensure that the collection agencies implement the collection strategy, help them fine-tune it where necessary to encourage complementary collection strategies, and seek to avoid redundant efforts.

As our case studies suggest, there will likely be conflicts over resources. For instance, the Mission Manager for Terrorism may argue that more satellite time should be directed toward targets of interest in Country Y, and the DNI's designee will be forced to make hard choices. The Mission Manager and the DNI's appropriate deputy will remain involved in the day-to-day monitoring of collection efforts to coordinate with the collection agencies and ensure that Country X issues are addressed—or that an inability to collect on the Country X target, due to a need to focus collection resources elsewhere, is factored into Community-wide assessments.

Integrated Data Management

The collection enterprise does not stop with the actual collection of information. It is also about moving that information into the collection agencies, processing and exploiting the data, disseminating it to analysts and, increasingly, directly to users. All of this requires a sophisticated information infrastructure that allows for the manipulation of huge volumes of data. (Chapter 9 (Information Sharing) deals with the necessity of removing barriers to information

flow *among* agencies.) But a precondition to improving Community-wide information sharing is the development of common data management infrastructures *within* individual agencies that can be integrated with the Community as a whole. Only then will different collection agencies be able to collaborate and effectively maximize the advantages of multi-discipline collection.[11]

The idea that an integrated data management infrastructure will allow collection agencies to work more closely with one another is far from new. In fact, we must commend the current Directors of NSA and NGA—Lieutenant General Michael Hayden and Lieutenant General (Ret.) James Clapper—for their visionary efforts to create interfacing data management tools and methodologies for their two agencies. Regrettably, the directors' efforts have been stymied by two problems. First, the agency bureaucracies have tended to focus on their local needs versus the more global, Community-wide needs. Second, both agencies have been unable to successfully complete the necessary large-scale acquisition contracts.[12]

The lack of progress in developing new information infrastructures, and the failure to develop common information technology standards across the Community, will continue to be a major impediment to an integrated collection enterprise. Without a Community-wide plan, we fear that individual agencies will continue to invest—and waste—large amounts of resources in underperforming information infrastructures that cannot be integrated easily with other information systems across the Community.

We therefore propose, consistent with the *Intelligence Reform and Terrorism Prevention Act's* directive,[13] that the DNI develop a strategic plan for enabling collaboration and information sharing among collection agencies. This plan would identify the requirements for a Community-wide information infrastructure, set common standards for promoting information sharing techniques such as data-tagging, and develop guidance on new tools and methods for exploiting and processing collected data.

Integrated Strategic Planning and Investment

Technical collection currently accounts for roughly half of the intelligence budget.[14] One of the obstacles to achieving an integrated collection system is the fragmented nature of the intelligence budget, which is divided along pro-

grammatic lines and largely committed to legacy systems. Previous attempts to develop Community-wide budget priorities have met resistance from individual intelligence organizations, which naturally prefer the autonomy they enjoy under the current system.

Without a single individual or office to overcome these barriers, the Intelligence Community's enormous investment in technical collection has been, in some cases, duplicative and slow to respond to changed conditions; it has also provided the United States with inadequate capabilities to penetrate targets. Integrating strategic planning and investment would give a single office authority to look across collection agencies and advise the DNI on where to invest the Community's resources.

We believe the DNI should establish an office with requisite authorities to develop a strategic investment plan for Community-wide collection capabilities. This body would:

- Review, evaluate, and oversee National Intelligence Program (NIP) collection programs and budgets as part of the DNI's annual review process, including strategic investment for development of future collection concepts and associated processing, exploitation, and analysis capabilities;

- Conduct evaluations of collection investment alternatives across disciplines;

- Allocate strategic investments to develop new sources and methods;

- Collaborate with designees of the Secretary of Defense to ensure the effective integration of collection systems in the NIP, Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA) budgets;

- Ensure that investments in collection, processing, exploitation, and dissemination technologies are appropriately balanced; and

- Ensure appropriate funding for strategic investment priorities and, to the extent possible, ensure that such funds are not obtained through supplemental funding.

Integrated Development of New Collection Techniques

The primary obstacle to developing and implementing a sound research and development program is the same as that which stands in the way of an integrated strategic investment plan. Today there is no single official empowered to manage the Community's overall research and development needs. A single person should have authority to assess alternative options, select among competing priorities, choose solutions, and direct appropriate research and development initiatives to solve collection problems.

To establish an integrated approach to research and development across the Intelligence Community, the DNI should create an office responsible for assessing collection technology needs and developing a unified research and development strategy. This structure should be responsible for the following functions:

- Assessing program and technology gaps and proposing solutions;
- Developing and defining collection research and development strategies and plans;
- Developing and implementing innovative approaches for technical, operational, and exploitation functions related to collection;
- Working with the Office of the DNI's Director of Science and Technology to ensure that the national technology community—including the government, national labs, academia, and the commercial sector—has effective processes to recognize future threats and opportunities, and to help develop new and effective collection approaches;
- Ensuring the development of collection sensors, platforms, systems, and architectures that show substantial promise of defeating foreign denial and deception programs; and
- Ensuring that agencies have sufficient research and development funds to take advantage of innovative new approaches in collection and analysis.

This office should also be equipped with a significant budget in order to fund independent research without first seeking consensus from the collection agencies' various research and development units. It should also be given

authority to oversee and recommend modifications to the research and development budgets of those units. We believe that the DNI should determine how these collection-specific research and development needs should relate to the newly-created Director of Science and Technology. [15]

Even with the creation of an office dedicated to Community-wide research and development, we remain concerned that the DNI may have difficulty ensuring unity of effort.[16] The DNI does not have control over significant portions of the research and development budget contained in JMIP and TIARA. Nor does the new legislation resolve existing conflicts between the authorities of the DNI and Secretary of Defense for funding and managing programs within the NIP, JMIP, and TIARA. We have learned of several instances in which important efforts were stalled by conflicts of authority. For example, at least one major technical collection initiative—one that we cannot describe in our unclassified report—has been in limbo for over two years because the Intelligence Community and Defense Department cannot agree on a single set of requirements, mission scenarios, funding, operational control, and integration with other technical collection programs. Our recommendation, therefore, is only a half-step toward the needed solution; as we have noted elsewhere (see Chapter 6, Management), close cooperation with the Defense Department is also required.

IMPROVING THE PERFORMANCE OF INDIVIDUAL COLLECTION DISCIPLINES

Human Intelligence Collection

Human intelligence serves policymakers by providing a unique window into our targets' most guarded intentions, plans, and programs. During the Cold War, intelligence from GRU Colonel Oleg Penkovskiy proved critical to our management and eventual resolution of the Cuban missile crisis. Later, Polish Colonel Ryszard Kuklinsky provided us with highly secret war plans from the Soviet Union. The recent penetration of the A.Q. Khan nuclear proliferation network is another example of an impressive human intelligence achievement.

As the President himself has observed, the United States desperately needs human sources to confront today's intelligence challenges.[17] To its credit, the Intelligence Community has, since September 11, undertaken efforts to rise to

the President's challenge and redirect human intelligence collection toward today's threats. But as our case studies make clear, in the context of hard targets like Iraq, Iran, North Korea, and al-Qa'ida, human intelligence is still not delivering the goods. We have identified numerous reasons for this:

Losing human intelligence resources. Since the dissolution of the Soviet Union, the loss of human intelligence resources has brought the Community well below optimal strength. In the 1990s, CIA's Directorate of Operations (DO) experienced an appreciable decline in its career service rolls, including a significant decline in operations officers.[18] Similarly, DIA's Defense HUMINT service lost hundreds of billets between 1995 and 2001.[19] The Community has suffered a hemorrhage of irreplaceable experience.

The threat has changed, but we have not adapted. Post-Cold War targets—which include numerous "denied areas" and elusive non-state terror organizations—require our human intelligence agencies to develop different skill sets. We believe that human intelligence collectors have been too slow to respond to this sea change in operational requirements.

The hardest conventional targets remain largely impenetrable. Traditional state targets remain resistant to human penetrations. Our foes tend to be police states and totalitarian dictatorships—regimes that typically excel at countering espionage against them. Closed states like North Korea and Saddam Hussein's Iraq have countered U.S. collection efforts with, among other tools, pervasive counterintelligence and security apparatuses. Our case studies—including both Iraq (Chapter 1) and our classified studies of other "closed societies"—starkly illustrate human intelligence collectors' continuing difficulty in penetrating these targets. Intelligence Community coordination issues, bureaucratic risk aversion, and highly inadequate cover diversification have all retarded progress against these key targets.

Human intelligence collection is uncoordinated and lacks common standards. Minimal coordination among elements in the past sufficed when the CIA, FBI, and the Defense Department had more distinct missions, but lines of authority have blurred due to these agencies' responses to the imperatives of the terrorist threat. Both the FBI and the Defense Department's Special Operations Forces are major new players, and DIA has expanded its existing human intelligence service. There is considerable value in the new resources

and perspectives that these new players bring, but there are risks as well. These risks can only be addressed through greater coordination.

Some human intelligence agencies do a poor job of validating human sources. The story of "Curveball"—the human source who lied to the Intelligence Community about Iraq's biological weapons programs—is an all-too-familiar one. Every agency that collects human intelligence has been burned in the past by false reporting; indeed, the Intelligence Community has been completely fooled several times by large-scale double-agent operations run by, among others, the Cubans, East Germans, and Soviets. It is therefore critical that our human intelligence agencies have excellent practices of validating and vetting their sources.

We believe that these deficiencies in validating sources demonstrate that the Intelligence Community needs to change fundamentally the way it conducts the human intelligence mission. Specifically, we recommend: (1) that the Community develop and increase the use of new human intelligence collection methods; (2) that a new Human Intelligence Directorate be created within the CIA and that it be given the lead in coordinating the full spectrum of human intelligence activities performed Community-wide; (3) that steps be taken to professionalize the Intelligence Community's cadre of human intelligence officers; and (4) that human intelligence training be diversified and expanded to broaden expertise and reduce seemingly intractable training bottlenecks.

Coordinating Human Intelligence

Recommendation 3

Strengthen the CIA's authority to manage and coordinate overseas human intelligence operations across the Intelligence Community by creating a Human Intelligence Directorate outside the Directorate of Operations.

The new Act stipulates that the Director of the Central Intelligence Agency (DCIA) will "provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community … and ensure that the most effective use is made of resources."[20] Consistent with this statutory mandate, we recommend the creation of a Human Intelligence Directorate—within the CIA

but separate from the existing Directorate of Operations—to serve as a national human intelligence authority, exercising the responsibility to ensure the coordination of all agencies conducting human intelligence operations on foreign soil.

The Human Intelligence Directorate would have direct "command" authority over CIA human intelligence components—which, if this Commission's recommendations are accepted, would be expanded to include not only the Directorate of Operations but also the proposed Innovation Center discussed in the following section. But its overseas human intelligence coordination responsibilities would extend more broadly across the Intelligence Community.

When most people think of human intelligence, they think about the CIA—and, more specifically, about the professional case officers in the CIA's Directorate of Operations (DO) who conduct the CIA's human espionage operations. But there are in fact a host of entities that collect human intelligence either through clandestine or overt means, ranging from long-established agencies like the Defense HUMINT service and the FBI to agencies that until recently had not viewed themselves as intelligence collectors (like immigration officials and customs officers). This range of entities conducting human intelligence activities, of course, raises serious coordination challenges—and these challenges are only becoming more formidable. As we discuss in Chapters Six (Management) and Ten (Intelligence at Home), both the Defense Department and the FBI are stepping up their own, more traditional overseas intelligence activities, as well as other, less conventional human intelligence efforts, such as those associated with the Department of Defense's special operations forces. While we believe that many of these efforts are commendable, they heighten the risk that intelligence operations will be insufficiently coordinated—a state of affairs that can, in the world of foreign espionage, have dangerous and even fatal consequences.

We propose the creation of the Human Intelligence Directorate within CIA to address this pressing need. The Directorate would coordinate the overseas operations of the DO with those of the Defense Department and the FBI. The CIA—with a network of case officers around the globe—is uniquely situated to perform this function, and its power to insist on such coordination should be reaffirmed. To accomplish this task, however, there are many issues the CIA's Human Intelligence Directorate will have to resolve with the Defense

Department and the FBI in establishing its authorities with respect to human intelligence. In order to ensure suitable attention to this process, we recommend the Director of CIA (DCIA) be required to report to the DNI, within 90 days of the DNI's confirmation, exactly what protocols have been established with the Defense Department and the FBI to ensure effective coordination among the three organizations and appropriate oversight of their respective activities.

The need for coordination is pressing and pronounced. Increasingly, for example, the FBI's intelligence operations cross national boundaries, thus requiring greater coordination with CIA and the Defense Department. The CIA, and in particular its field supervisors, should act as the focal point for overseas coordination to ensure that FBI tradecraft practices abroad reflect the hostile environment in which intelligence gathering occurs.

We emphasize three things that would *not* occur under our proposed system. First, other human intelligence collection agencies—to include DIA clandestine and overt operations, the Special Operations Command, and other human intelligence operations carried out by military services—would not surrender command authority and operational control over their human intelligence assets. Rather than "run" these components, the Human Intelligence Directorate would broadly direct and coordinate human intelligence activities overseas. Second, the DCIA's authorities as head of the Human Intelligence Directorate would not extend to directing collection against any specific target; rather, as discussed earlier in this Chapter and in Chapter Eight (Analysis), this responsibility would fall to Mission Managers. Third, we do not propose changing or stifling successful coordination efforts that already occur at "lower levels" in the field.

In addition to coordinating overseas human intelligence operations for the Community, the Human Intelligence Directorate would serve as the centerpiece for Community-wide human intelligence issues, including by helping to develop a national human intelligence strategy, integrating (where appropriate) collecting and reporting-disseminating systems, and establishing Community-wide standards for training and tradecraft. Finally, the Directorate also would have the responsibility for expanding, enriching, and diversifying the full range of human intelligence capabilities. We believe it is this task that makes it essential that the Human Intelligence Directorate be located within the CIA and under the direction of the Agency's Director—but *not* part of the

Directorate of Operations. As discussed in detail below, we believe that the DO is not ideally situated to incubate a variety of new human intelligence techniques, or to vet those developed by other agencies or entities, such as the Innovation Center.

Fostering Innovation

Recommendation 4

The CIA should develop and manage a range of new overt and covert human intelligence capabilities. In particular, a "Human Intelligence Innovation Center," independent of the CIA's Directorate of Operations, should be established to facilitate the development of new and innovative mechanisms for collecting human intelligence.

The Directorate of Operations, which conducts the CIA's human espionage operations, is one of the Intelligence Community's more elite and storied organizations. It takes justifiable pride in its ability to recruit spies and manage diplomatically delicate foreign liaison relationships. The DO has rigorous training programs—its premier training facility known colloquially as "the Farm," has become well-known through its depiction in popular movies and novels—and continues to attract some of the nation's most impressive talent.

It is a well-known rule of bureaucratic behavior, however, that when an organization does something particularly well, it is difficult to encourage that organization—or the people within it—to do things that are new and different.[21] And so it has proven with the Directorate of Operations. While the need to develop new methods of collecting human intelligence has been apparent for years, the DO has struggled to develop and "mainstream" new techniques, remaining wedded instead to the traditional model of recruiting spies.

We have seen positive indications that the new leadership of the CIA is aggressively exploring new human intelligence methods. If it is left to the DO to develop and implement these new ideas, however, we are skeptical that they will ever become more than a peripheral part of the DO's mission. Accordingly, we recommend the establishment of an "Innovation Center" within the CIA—but *not* within the Directorate of Operations—responsible for oversee-

ing the development of new and non-traditional methods of conducting human intelligence. This center's mission would be not only to evaluate and develop new human intelligence approaches, but also to serve as a think-tank and proving ground for new human intelligence techniques and methods. [22]

We recognize that there are arguments that such an innovation center should be placed outside of the CIA entirely, in light of the historically outsized influence that the DO has held over the CIA's management. But in our view it would be inadvisable to add yet another organization to the already dispersed constellation of human intelligence collection entities. (Indeed, as we suggested in the previous section, we believe that the CIA should exercise a *stronger* hand in coordinating human intelligence collection across the Intelligence Community.) The DNI, however, should monitor the Innovation Center closely, not only to ensure that it is performing its mission well but also to encourage the implementation of its useful new ideas.

In addition to this institutional recommendation to encourage the development of innovative new human intelligence practices, in our classified report we also point to several specific methods that in our judgment should either be explored or used more extensively. Unfortunately, these specific methods cannot be discussed in our unclassified report.

Professionalizing Human Intelligence Across the Community

We have been critical of the CIA's Directorate of Operations at certain points, but it is important also to emphasize what they do well. While we have concluded that the DO is not the best place to foster innovation in human intelligence, it does continue to set the standard for traditional human intelligence operational "tradecraft." It is to the DO that the rest of the Community should look for guidelines on asset validation and ways to build productive relationships with liaison services. We recommend that the DCIA, acting in his Community leadership role as the head of the Human Intelligence Directorate, work actively to develop and further professionalize human intelligence components outside of CIA in these and other areas.

For example, our review of the Community suggests that the Defense Department's attempts to develop a clandestine strategic intelligence arm have fallen short because of the absence of a professional human intelligence career path—for both military officers and civilians—and an overall environment that historically has not fostered sufficient respect for, or investment in,

human intelligence collection capabilities. While there are of course many talented Defense HUMINT clandestine case officers, the service has not developed the operational capability that it would possess if intelligence officers followed a long-term career path and passed on lessons learned.[23] We believe that the CIA—in its role as Community-wide human intelligence coordinator—should assist DIA in further professionalizing its cadre of clandestine case officers, and—in light of the Community-wide scarcity of fully-trained case officers—ensure that Defense HUMINT's clandestine service is properly leveraged and coordinated with the DO's operations.

Recommendation 5

The CIA should take the lead in systematizing and standardizing the Intelligence Community's asset validation procedures, and integrating them with all information gathering activities across the human intelligence spectrum.

The case of Curveball (described in detail in our Iraq study) illustrates the importance of integrating sound validation processes wherever possible—in all forms of human intelligence activities including unilateral collection, liaison-provided information, debriefings, and other human-acquired inputs into intelligence reporting. (By "validation processes" we mean the ways in which intelligence collectors ensure that the information provided to them is truthful and accurate.) The Pentagon's plans to increase its human intelligence capabilities make it especially important that Defense HUMINT adopt and institutionalize sound vetting and validation practices to ensure the reliability of information it disseminates to the Intelligence Community. It will be the responsibility of the Human Intelligence Directorate and the Defense Intelligence Agency to ensure that proper source validation occurs whenever possible, and that overt collectors are not simply passive conduits for human intelligence. In our classified report, we also make specific recommendations to improve the asset validation practices of human collection agencies that cannot be discussed in an unclassified format.

Collecting Human Intelligence: Custodial Interrogations

One source of critical intelligence, particularly with respect to terrorist plans and operations involving the use of nuclear, biological, or chemical weapons, is the interrogation of captured detainees. We consider it essential, and indeed have been assured that it is currently the case, that the Attorney General personally approves any interrogation techniques used by intelligence agencies that go beyond openly published U.S. government interrogation practices. While we recognize that public disclosure of Attorney General approved or forbidden techniques to be used by U.S. interrogators or by foreign personnel in interrogations in which the United States participates would be counterproductive, we emphasize that it is vital that all such practices conform to applicable laws. Where special practices are allowed in extraordinary cases of dire emergency, those procedures should require permission from sufficiently high-level officials to ensure compliance with overall guidelines, and records should be kept to provide oversight for deviation from regular practices. It is also important that notice of Attorney General approved techniques and the circumstances of any deviations from regular practices be given to appropriate congressional overseers. Interrogation guidelines should also form part of the training of relevant intelligence personnel. Compliance with approved practices should be uniformly enforced. Assurance that these steps have been taken across the Community will enhance the credibility of the Intelligence Community as a law-abiding and responsibly governed entity in the public mind, thereby enhancing its ability to perform its crucial functions.

Shaping the Force: A Larger and Better Trained Human Intelligence Officer Cadre

Recommendation 6

The Intelligence Community should train more human intelligence operators and collectors, and its training programs should be modified to support the full spectrum of human intelligence collection methods.

The reforms and initiatives discussed above would vastly improve our nation's human intelligence capabilities. But one thing will still be missing—the people necessary to do what needs to be done. We recognize the ease of saying "more money will solve the problem," and for that reason have avoided

recommendations that do little more than propose an outlay of additional funds. But in the case of human intelligence, we simply need more people.

In our classified report, we offer statistics showing how badly outgunned our human intelligence collectors are, at precisely the time when the most is expected of them. Although we make few recommendations that we believe will require substantial budget increases, we do believe that this is an area where increased funding for the purpose of expanding human intelligence forces would be appropriate—and where, as we have noted elsewhere (see Management, Chapter 6), the need for long term planning militates strongly toward a shift away from unpredictable supplemental budget appropriations. In our classified report, we offer additional recommendations on how to improve human intelligence training programs within the Intelligence Community. This discussion cannot be included in our unclassified report.

Technical Intelligence Collection

Signals and Imagery Intelligence

Signals intelligence and imagery collection systems are obviously critical to the Intelligence Community's ability to collect information. Unfortunately, as our Iraq case study vividly illustrates, a combination of factors—most relating to our adversaries' increasingly effective use of denial and deception—have significantly eroded the utility of the Community's legacy signals and imagery systems. In our classified report, we specify examples highlighting the scope of the problem.

The Community is investigating and developing numerous technologies and methods that can potentially surmount some of these collection challenges. These technologies cannot be discussed in detail in an unclassified report. However, we recommend that the DNI should, as an early priority, delve into the complex technical issues that surround these innovations. The DNI should also assist collectors in developing and operationalizing the most promising innovations, while redoubling efforts to improve *existing* means of countering and reducing the distorting effects of denial and deception.

To aid him in the latter effort, the DNI will inherit a commendable roadmap previously developed by the DCI. Among other things, this strategy establishes efforts to counter-denial and deception by our adversaries as "a top priority for the Intelligence Community."[24] Yet, like many DCI strategies, we are

concerned that the prose has not fully translated into practice. To ensure effective implementation, we suggest a mid-course review of the strategy's first five years: a thorough examination of accomplishments and shortfalls, an update of the principal actions that specific Intelligence Community entities have taken and should take, and a renewed effort to solicit the full backing and resources of relevant planning and acquisition professionals across the Community. The effort to overcome foreign denial and deception will be ongoing; there is no easy or quick fix for the problems that plague technical collectors.

In the short term, technical collectors' most important contributions to the Community's mission may occur when they operate in conjunction with other collection disciplines. As a result, we believe that implementation of the integrated collection enterprise we recommend in this chapter will significantly enhance the Community's ability to optimize its existing technical collection capabilities. Target Development Boards, in particular, will provide an ongoing opportunity to engage in cooperative collection efforts among collection disciplines—specifically to capitalize on the joint capabilities of technical and human collectors. Such joint activities have been at the source of some of the Community's most notable successes in recent years. In our classified report, we cite examples of types of joint efforts which we cannot discuss here.

Signals Intelligence in the United States

Recommendation 7

The President should seek to have the Foreign Intelligence Surveillance Act amended to extend the duration of electronic surveillance and "pen registers" in cases involving agents of foreign powers who are *not* U.S. persons.

The Foreign Intelligence Surveillance Act (FISA)[25] governs, in part, the manner in which the U.S. government may conduct electronic surveillance within the United States and electronic surveillance of U.S. persons abroad. NSA and the FBI have long operated within the confines of FISA and—according to NSA—the statute has not posed a serious obstacle to effective intelligence gathering. It has, however, become a growing administrative burden, because NSA (in cooperation with the FBI) must now obtain far more FISA warrants than it did when traditional communications were prevalent.[26]

The increased frequency with which NSA must obtain FISA orders, in turn, has placed a significant burden on the Department of Justice's Office of Intelligence Policy Review (OIPR), which represents the United States in the Foreign Intelligence Surveillance Court when NSA requires a FISA order.

We recommend that the President seek to have FISA amended to extend the duration of electronic surveillance and "pen register"[27] orders as they apply to agents of foreign powers who are *not* U.S. persons. We think the President might consider seeking an extension of the initial electronic surveillance period from 90 to 120 days, as well as an extension from 120 days to one year for follow-on orders. In addition, we recommend seeking an extension of the initial pen register period from 90 days to one year. Again, it is our view that each of these extensions should only apply to non-U.S. persons; by limiting the extension in this manner, the Justice Department and the FISA Court will maintain their current levels of attention when U.S. persons' civil liberties are implicated. Although these relatively modest changes to FISA procedures will not eliminate the burdens carried by NSA and the Department of Justice, we believe that they will at least lessen them and allow those agencies to focus their attention where it is most needed.

Measurement and Signature Intelligence

Recommendation 8

The DNI should appoint an authority responsible for managing and overseeing innovative technologies, including the use of technologies often referred to as "MASINT."

To its proponents, measurement and signature intelligence, or MASINT, is an unjustly overlooked specialty. A wide variety of collection techniques fall under the heading of MASINT—everything from sensors, lasers, ground-based radars, and pretty much any other technical measure that does not fit easily into the traditional intelligence disciplines.[28] Skeptics view these as a batch of unrelated technical intelligence tools, better developed and funded separately rather than under a single label.

Putting aside these definitional problems, some MASINT technical collection measures have had successes. Such technical capabilities can some-

times identify WMD programs, and can help counter denial and deception programs.

Although we are unsure of exactly how such techniques can best be supported, we are confident that the current situation is not the answer.[29] The designation of DIA—which lacks the staff, budget, and authority to control the development and deployment of MASINT systems—as the "National MASINT Manager" has failed to help these techniques prosper. These techniques are, almost by definition, some of the more innovative collection techniques in the Intelligence Community's arsenal, but they are often given short shrift as a result of DIA's neglect or disinterest.

We therefore recommend that the DNI take responsibility for coordinating new intelligence technologies, including those that now go under the title MASINT. This could be done by a special MASINT authority or as part of the DNI's Office of Science and Technology.

It is critical to note that, in our view, the MASINT coordinator should *not* directly control MASINT collection. Rather, we believe the most sensible division of MASINT responsibilities is that NGA be responsible for imagery-derived MASINT, while CIA and Defense Department elements take responsibility for their own operational sensors and other aspects of MASINT that fall naturally into their bailiwicks. At the same time, the DNI's designated representative would monitor the status of MASINT-like programs throughout the Intelligence Community to ensure that they are fully implemented and given the necessary attention.

Open Source Collection

Recommendation 9

The DNI should create an Open Source Directorate in the CIA to use the Internet and modern information processing tools to greatly enhance the availability of open source information to analysts, collectors, and users of intelligence.

Open Source information has long been viewed by many outside the Intelligence Community as essential to understanding foreign political, economic, social, and even military developments.[30] Currently, the Intelligence Commu-

nity has one collection organization, the Foreign Broadcast Information Service (FBIS), that specializes in providing some of these vital elements—particularly the rapid reporting of foreign print, radio, and television news. While this service is highly valued within the Community and academia, the Community does not have any broader program to gather and organize the wealth of global information generated each day and increasingly available, if only temporarily, over the Internet.

We also believe that the need for exploiting open source material is greater now than ever before. Today, the spread of information technology—and the ever increasing pace at which it advances—is immune to many traditional, clandestine methods of intelligence collection. Whereas advanced technological research once occurred only in large facilities and within enormous government bureaucratic institutions, today it can (and does) occur in nondescript office parks or garages, and with very small clusters of people. And for these new challenges, many open source materials may provide the critical and perhaps only window into activities that threaten the United States.

Much has happened in the world of open source in the past ten years. Internet search tools like Google have brought significant new capabilities and expectations for open source information to analysts and users alike. Regrettably, the Intelligence Community's open source programs have not expanded commensurate with either the increase in available information or with the growing importance of open source data to today's problems. This is an unacceptable state of affairs. Consider the following:

- ***The ever-shifting nature of our intelligence needs compels the Intelligence Community to quickly and easily understand a wide range of foreign countries and cultures.*** As we have discussed, today's threats are rapidly changing and geographically diffuse; it is a fact of life that an intelligence analyst may be forced to shift rapidly from one topic to the next. Increasingly, Intelligence Community professionals need to quickly assimilate social, economic, and cultural information about a country—information often detailed in open sources.

- ***Open source information provides a base for understanding classified materials.*** Despite large quantities of classified material produced by the Intelligence Community, the amount of classified information produced on any one topic can be quite limited, and may be taken out of

context if viewed only from a classified-source perspective. Perhaps the most important example today relates to terrorism, where open source information can fill gaps and create links that allow analysts to better understand fragmented intelligence, rumored terrorist plans, possible means of attack, and potential targets.

- ***Open source materials can protect sources and methods.*** Sometimes an intelligence judgment that is actually informed with sensitive, classified information can be defended on the basis of open source reporting. This can prove useful when policymakers need to explain policy decisions or communicate with foreign officials without compromising classified sources.

- ***Only open source can "store history."*** A robust open source program can, in effect, gather data to monitor the world's cultures and how they change with time. This is difficult, if not impossible, using the "snapshots" provided by classified collection methods.

We believe that this gap between the Intelligence Community's needs and its capabilities must be addressed on two fronts: collection and analysis. The former we discuss here; the latter is discussed more fully in Chapter Eight (Analysis).

We recommend that the DNI create an Open Source Directorate in the CIA to develop and utilize information processing tools to enhance the availability of open source information to analysts, collectors, and users of intelligence. At a minimum, such a program should gather and store many, if not most, of the digital newspapers and periodicals available over the Internet, regardless of language. (Daily storage is required because most of these newspapers and periodicals are on the Internet for only short periods of time.) We believe that this open source information will be invaluable to those charged with watching emerging threats and would provide a baseline for intelligence collectors and analysts when issues suddenly rise to national security significance. In addition, it can tip off analysts and collectors to changes that warrant more focused intelligence collection.

In the near term, we believe that without an institutional "champion" and home, open source will never be effectively used by the Intelligence Community. It is our hope that open source will become an integral part of all intelli-

gence activities and that, at some point in the future, there may no longer be a need for a separate directorate. We acknowledge that our recommendation could create one more collection specialty. But, for now, open source is inadequately used and appreciated and is in need of the high-level, focused attention that only a separate directorate can provide.

As important as collecting open source material, however, is the task of getting the material to the analysts who need it. We were repeatedly told that analysts have difficulty accessing open source information at their desks.[31] The Intelligence Community must make a concerted effort to solve the technology and security challenges associated with getting open source information to every analyst's desktop.

PROTECTING SOURCES AND METHODS

Our case studies strongly suggest that a persistent inability to protect human and technical collection sources and methods has substantially damaged U.S. intelligence capabilities. Authorized and unauthorized disclosures have compromised critical signals interception and satellite imagery programs, as well as hard-earned human intelligence sources. Better protection of these sources and methods, which should be thought of as the Community's crown jewels, will require sustained attention by the DNI and the consideration of a range of possible approaches. We believe that the act's emphasis on the DNI's obligation to protect sources and methods will help raise the priority placed on this important issue.[32] We also believe that the institutional recommendations in our information sharing chapter (Chapter 9)—which include making a single person in the office of the DNI responsible both for information sharing and for information security—will help ensure that information sharing imperatives do not overwhelm the need to protect sources and methods.

To accompany these institutional suggestions, we offer recommendations to help address two problems that have harmful effects on sources and methods: (1) the problem of *authorized* disclosures and (2) the problem of *unauthorized* disclosures (more commonly referred to as "leaks") of classified information.

Authorized Disclosures of Sources and Methods

Recommendation 10

Efforts should be taken to significantly reduce damaging losses in collection capability that result from *authorized* disclosures of classified information related to protection of sources and methods.

Authorized disclosures often have unintended and harmful effects. One common source of such disclosures is the sharing of intelligence with foreign countries both through cooperative ventures and diplomatic demarches. The Intelligence Community should take more rigorous steps to integrate counterintelligence expertise into the sharing and demarche decisions and processes, and to formally analyze the potential costs and benefits of such disclosures. These processes would need to include methods for tracking the consequences of unauthorized disclosures, and a formal process for resolving disputes among agencies and stakeholders over the costs and benefits of particular disclosure decisions.

Another *de facto* "disclosure" of information about the technical capabilities of intelligence satellites occurs when public announcements are made concerning a satellite launch. We therefore recommend that the United States examine whether its space launch techniques can be altered to shield spaceborne collection techniques and operations more effectively.

The Problem of Media Leaks

The scope of damage done to our collection capabilities from media disclosures of classified information is well documented. Hundreds of serious press leaks have significantly impaired U.S. capabilities against our hardest targets. In our classified report, we detail several leaks that have collectively cost the American people hundreds of millions of dollars, and have done grave harm to national security. We cannot, however, discuss them in an unclassified format. These and hundreds of other leaks have been reported to the Justice Department by the Intelligence Community in the last ten years. However, to date, not a single indictment or prosecution has resulted.

According to past government studies, the long-standing inability of the U.S. government to control press leaks results from a combination of fac-

tors—the use of unauthorized disclosures as a vehicle to influence policy, the lack of political will to deal firmly and consistently with government leakers in both the executive and legislative branches, the difficulty of prosecuting cases under existing statutes, and the challenge of identifying the leaker.[33] The government's impotence in dealing effectively with this problem was well characterized by then-Deputy Assistant Attorney General Richard K. Willard, in 1982:

> In summary, past experience with leaks investigations has been largely unsuccessful and uniformly frustrating for all concerned….The whole system has been so ineffectual as to perpetuate the notion that the Government can do nothing to stop the leaks.[34]

The Commission recognizes the enormous difficulty of this seemingly intractable problem and has considered a broad range of potential solutions. We conclude that the long-standing defeatism that has paralyzed action on this topic is understandable but unwarranted. Leaks cannot be stopped, but they can be reduced. And those responsible for the most damaging leaks can be held accountable if they can be identified and if the government is willing to prosecute them.

Recommendation 11

The DNI should ensure that all Inspectors General in the Intelligence Community are prepared to conduct leak investigations for their agencies; this responsibility can be coordinated by a Community-wide Inspector General in the Office of the DNI, if such an office is established.

Coordinated leaks investigations. The DNI Inspector General, assuming one is named, should be given specific responsibility for overseeing leaks investigations within the Intelligence Community and for coordinating investigations that require reaching into multiple agencies within the Community. The DNI's Inspector General would be uniquely positioned to coordinate leak investigations across the Intelligence Community. Several intelligence agencies have explained that the Justice Department is rarely willing to open investigations of leaks when the number of possible leakers is large. Furthermore, these agencies have expressed the opinion that complaining agencies should be allowed to conduct investigations of their own employees so as to

narrow down the list of possible leakers. By heeding these concerns, this recommendation will reduce the investigative load for the Justice Department and FBI while putting more of the burden on the agencies that often feel the impact of leaks most directly.

Vigorous application of DNI administrative authorities. When internal CIA leakers have been identified, the DCI's authority to impose sanctions ranging from fines, suspension or revocation of clearances, or even firings is relatively robust. This authority should extend to the DNI. The DNI should, in turn, vigorously enforce the 2002 DCI Directive on stemming unauthorized disclosures across the Community.[35] We hope that the 2002 Directive will acquire greater force under the new DNI than it has had under past DCIs.

Better education and training for intelligence producers, users, and media. Policymakers who leak intelligence to the press in order to gain political advantage and journalists who publish leaked intelligence may do so without fully appreciating the potential harm that can result to sources and methods. The Intelligence Community should consider implementing a widespread, modern-day equivalent of the "Loose Lips Sink Ships" campaign to educate individuals about their legal obligations—and possible penalties—to safeguard intelligence information. Officers at all agencies that produce and use intelligence should be fully briefed at the time they first sign the non-disclosure agreement and be periodically re-briefed about its responsibilities.

Internal changes at the Department of Justice. As noted more fully in Chapter Ten (Intelligence at Home), we recommend that the primary national security component of the Department of Justice be placed under the auspices of a single Assistant Attorney General. We do so in the hope that the combined forces of the Department can be better brought to bear on a variety of issues, including unauthorized disclosures.

Finally, there is one point regarding leaks on which the Commission could not come to agreement. During our work, we were repeatedly told that the greatest barrier to prosecuting leaks was in identifying the "leaker." And many people with whom we spoke also said that the best (if not only) way to identify leakers was through the reporters to whom classified information was leaked. In this vein, we thoroughly discussed the advantages and disadvantages of creating some sort of qualified privilege for reporters, which might simultaneously protect both First Amendment interests and the government's interest in protecting

classified information. Regrettably, and despite all of our efforts, we could not reach agreement on the details of such a proposal.

ENDNOTES

[1] Although the National Imagery and Mapping Agency (NIMA)—renamed the National Geospatial-Intelligence Agency (NGA)—was established after the Cold War, it was cast from the same mold.

[2] CIA, Title Classified (OTI IA 2002-141) (Aug. 26, 2002); CIA, Title Classified (OTI IA 2002-053 (SPS)) (Oct. 2004); CIA, Title Classified (OTI IA 2003-06) (Feb. 2003); Department of Defense Joint Staff, Title Classified (Dec. 2003); Defense Science Board, *Future Strategic Strike Systems* (Feb. 2004).

[3] National Intelligence Council (NIC), Title Classified (NIE 98-04) (1998-99).

[4] For a more detailed discussion of this issue, see Chapter Thirteen (Proliferation).

[5] NIC, Title Classified (NIE 98-04) (1998-90) at Volume 1.

[6] CIA, *The Jeremiah Report: The Intelligence Community's Performance on the Indian Nuclear Tests* (June 1, 1998) (hereinafter "Jeremiah Report").

[7] CIA, *Response to WMD Commission Request # 74* (Oct. 8, 2004).

[8] House Permanent Select Committee on Intelligence, IC21: *Intelligence Community in the 21st Century* (April 9, 1996) (hereinafter "IC21"); Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996) (hereinafter "Aspin-Brown Commission"); Jeremiah Report.

[9] *See, e.g.*, IC21.

[10] Target Development Boards would not just address analysts' needs. They would also address the needs of the military commanders for intelligence support to military operations.

[11] This idea is not unlike the Department of Defense's theory of Network Centric Warfare, which allows for widespread dissemination of data to the military to provide a shared awareness of the battle space. *See generally* Congressional Research Service, *Network Centric Warfare: Background and Oversight Issues for Congress* (June 2, 2004).

[12] Here we cite an example of an NSA acquisition problem that cannot be included in our unclassified report.

[13] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-458 (hereinafter "IRTPA").

[14] This includes the tactical programs in the Department of Defense. FY2005 NFIP, JMIP, and TIARA Congressional Budget Books.

[15] IRTPA at § 1011.

[16] We recognize that some competition in research and development is desirable and should be encouraged by the DNI. At the same time, even when research and development occurs in several locations, its efforts must still be integrated in a way that minimizes unproductive redundancy.

[17] *See, e.g.*, Memorandum from the President to the Director of Central Intelligence (Nov. 18, 2004).

[18] CIA, Directorate of Operations Recruitment (Sept. 14, 2004) (briefing slides).

[19] Interview with Defense HUMINT officials (Sept. 9, 2004).

[20] IRTPA at § 1011.

[21] *See generally* James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (Basic Books) (1989).

[22] If the innovation center proves a successful model, we believe the DNI should explore replicating it in other agencies as well.

[23] As we have already noted, we are far from the first to recognize the shortcomings in Defense HUMINT. *See, e.g.*, Aspin-Brown Commission; Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence* (1996); IC21; Defense Science Board *Task Force on Intelligence Support to the War on Terrorism* (Oct. 2003); House Permanent Select Committee on Intelligence, *Classified Annexes to The Intelligence Authorization Act For Fiscal Year 1998, 1999, 2003, 2004, 2005*.

[24] DCI, Title Classified (March 2000) at pp. 1-2.

[25] 50 U.S.C. §§ 1805, 1842.

[26] Interview with representatives of NSA's General Counsel's Office (Sept. 16, 2004); Interview with representatives of the Office of Intelligence Policy Review, Department of Justice (Oct. 25, 2004).

[27] A "pen register" or "trap and trace" device is roughly equivalent to using "caller identification" on a target phone (*i.e.*, it collects incoming and outgoing phone numbers).

[28] The term "MASINT" was first coined in 1970 by DIA to describe any number of disparate forms of collection and analysis such as active radar interrogation of targets, laser intelligence, optical measuring of reflected light from distant objects such as spacecraft, nuclear intelligence, acoustic intelligence, and infra-red analysis.

[29] According to DCI Porter Goss, "[p]ast efforts to manage MASINT have been hampered by an unrealistic view of MASINT as a single enterprise." Porter Goss, Director of Central Intelligence, *Cooperative Way Forward on MASINT Management* (Dec. 15, 2004) at p. 1.

[30] "Open Source" usually refers to all information that is generally publicly available and unclassified. It can include print media as well as radio and television broadcasting. With the advent of the Internet, there has been a major increase in the availability of open source textual data. This report focuses on, but is not limited to, this easily accessible open source textual data.

[31] *See, e.g.*, Interview with senior In-Q-Tel official (Feb. 3, 2005).

[32] The act states that the new DNI "shall protect intelligence sources and methods from unauthorized disclosure." It also limits the DNI's ability to delegate responsibility for protecting sources and methods, stating that the DNI "may only delegate" this authority to the Principal Deputy DNI. IRTPA at § 1011.

[33] National Counterintelligence Policy Board, *Report to the NSC on Unauthorized Media Leak Disclosures* (March 1996) at pp. C2-C4.

[34] *Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information* (March 31, 1982).

[35] DCI, Title Classified (Dec. 9, 2002).

CHAPTER EIGHT
ANALYSIS

Summary & Recommendations

The role of intelligence analysts is to tell policymakers what they know, what they don't know, what they think, and why. When analysts fail to provide adequate warnings of an impending threat, or provide incorrect conclusions to decisionmakers—as they did with Iraq—the consequences can be grave. Although there is no way to ensure against all future intelligence failures, we believe that several initiatives could improve management of analytic efforts, deepen analyst expertise, reduce intelligence gaps, and enhance the usability of existing information—all of which would improve the quality of intelligence.

Mission Managers, introduced in previous chapters, will play a critical role in this reform effort. They will encourage competitive analysis, present the views of all agencies to decisionmakers, ensure that analysts drive collection, and prepare the analytic community to meet the threats of the 21st Century.

In addition to adopting the Mission Manager approach, we also recommend—among other improvements—that the DNI:

- Emphasize strategic analysis by establishing a new long-term research and analysis unit, under the mantle of the National Intelligence Council, to serve as the lead organization for interagency projects involving in-depth analysis and expanded contacts with experts outside of the Intelligence Community;
- Institute Community-wide, career-long programs for training analysts and managers, and provide appropriate performance incentives;
- Develop and integrate into regular use new tools that can assist analysts in filtering the vast quantities of information that threaten to overwhelm the analytic process, as well as tools designed for foreign language exploitation; and
- Ensure that analysts are engaging in competitive analysis, mandate routine and ongoing examinations of finished intelligence, and require the lessons learned from "post mortems" to be incorporated into the intelligence education and training program.

INTRODUCTION

Analysts are the voice of the Intelligence Community.

While intelligence failures can certainly result from inadequate collection, recent experience shows that they can also occur when analysts don't effectively assess all relevant information and present it in a manner useful to decisionmakers. Improving the business of analysis should therefore be a major priority of the new Director of National Intelligence (DNI).

As in our chapter on collection, our recommendations—supported by vivid examples taken from our case studies—focus both on *integrating* analytical efforts across the Community and improving the overall *quality* of analysis.

The analytic effort in the Intelligence Community is hardly a monolithic enterprise; most of the Community's 15 organizations have at least one analytic component. Some of these agencies specialize in meeting the needs of particular users—notably the Defense Department's DIA and the State Department's INR. Some specialize in analyzing particular types of data—signals intelligence at NSA and geospatial intelligence at NGA. Some, such as the intelligence element of the Department of Energy, specialize in substantive intelligence topics, such as nuclear technology issues.

The separation of these analytic units serves a vital function; it fosters competitive analysis, encourages a diversity of viewpoints, and develops groups of analysts with different specialties. Any reform of the Community must preserve these advantages; our suggested move toward greater integration should not mean the homogenization of different viewpoints. Nevertheless, there is a great and growing need for Community analytic standards, interoperable and innovative technologies, access to shared information, and a common sense of mission. In many cases today, analysts in the 15 organizations are unaware of similar work being done in other agencies. Although analysts may develop working relationships with counterparts in other organizations, there is no formalized process or forum through which to do so. These dysfunctional characteristics of the current system must change; collaboration must replace fragmentation as the analytic community's primary characteristic.

Despite the fact that the analytic units are largely isolated and autonomous, we have been deeply impressed by pockets of excellence within them. The

Community is blessed with a highly intelligent, dedicated analytic workforce that has achieved significant successes. We also note that, in response to Iraq-related failures, the Intelligence Community has recently undertaken several serious (although scattered) efforts to improve the overall quality and integrity of its analytical methods and products.

We conclude, however, that these strengths and reforms are too few and far between. Our investigation revealed serious shortcomings; specifically, we found inadequate Intelligence Community collaboration and cooperation, analysts who do not understand collection, too much focus on current intelligence, inadequate systematic use of outside experts and open source information, a shortage of analysts with scientific and technical expertise, and poor capabilities to exploit fully the available data. Perhaps most troubling, we found an Intelligence Community in which analysts have a difficult time stating their assumptions up front, explicitly explaining their logic, and, in the end, identifying unambiguously for policymakers what they *do not know.* In sum, we found that many of the most basic processes and functions for producing accurate and reliable intelligence are broken or underutilized.

This Commission is not the first to recognize these shortcomings—we trod a well-worn path. Again and again, many of the same obstacles to delivering the best possible analytic products have been identified. The Church Committee's 1976 report, the House Permanent Select Committee on Intelligence's 1996 study of the Intelligence Community in the 21st Century, the 1998 Rumsfeld Report side letter to the President, the 1999 Jeremiah Report, the Markle Foundation's 2003 Task Force, and the 9/11 Commission Report all pointed to the problems created by the poor coordination and resistance to information sharing among Intelligence Community agencies. Some studies, notably the 1996 report by the Council on Foreign Relations and the 1996 study by the Aspin-Brown Commission, noted the need to systematically engage in and use competitive analysis. As early as 1949, the Hoover Commission faulted the Intelligence Community for failing to improve relations with decision-makers, and these concerns were echoed by the Aspin-Brown Commission and, most recently, the Markle Foundation Task Force.[1] Finally, the House and Senate intelligence committees have both noted the problems the Intelligence Community faces in processing the collected information available to it, as well as the difficulty analysts have engaging in long-term analysis, given the press of daily demands.[2]

In other words, many of the problems we have identified have been apparent to observers of the Intelligence Community—and to the Community itself—for decades. Nevertheless, they have remained largely unresolved, due largely to institutional resistance to change, the classified nature of the work, and a lack of political will to enforce change.

We believe the creation of the Office of the DNI offers a unique opportunity to finally resolve many of these issues by infusing the analytic culture with new processes and Community standards. We believe that this new management structure can foster a new sense of community among analysts. Until the analytic community adopts a new approach, analysts at one agency will continue to be denied access to critical reporting from others; analysts will resist collaborating and coordinating across units; managers will persist in placing the need to answer the "daily mail" over the need to develop true expertise; and new commissions will be appointed in the wake of future intelligence failures. As discussed in previous chapters, we believe that the creation of Mission Managers will be an important factor in avoiding this grim outcome.

Our recommendations, therefore, focus on exploiting the opportunity presented by the new legislation and the creation of the Office of the DNI, as well as on instituting changes to the Community's culture that will improve analytic performance. In doing so, we offer specific suggestions for how the community of analysts can be better integrated without sacrificing all-important independent analysis, and how the Intelligence Community can ensure that analysts have the tools, training, and "tradecraft" practices to ensure that the analytic community is prepared to meet today's and tomorrow's threats.

Achieving Community Integration Among Analysts

We believe that a principal goal of improving analysis should be to integrate the community of analysts while at the same time promoting independent—or competitive—analysis. In this sense, we believe a major challenge for the first Director of National Intelligence will be to foster more collaboration among analysts across the Community—that is, to bring the benefits of collaboration to daily support to the President, to strategic intelligence and warning, and to assistance to military, law enforcement, and homeland security efforts. In our view, there are five prerequisites to creating such a community:

Achieving Community Integration Among Analysts (Continued)

- ***Community standards*** for analysis (analytic expertise, analytic performance, and analytic presentation to consumers) so that the work of any one analytic unit can be relied upon and understood by others;
- ***A common analytic work environment*** (a shared network, compatible tools, and a common filing system for products and work in progress) so that a DNI can know the state of intelligence on critical issues, and so knowledge and supporting data can be shared quickly and efficiently across the Community;
- ***A group of "Mission Managers,"*** acting on behalf of the DNI, to oversee the state of intelligence on designated priority issues (including the state of analytic skills and resources, the gaps in existing knowledge, strategies to fill those gaps, and the effectiveness of agreed upon collection strategies)—from a Community perspective;
- ***A body of "joint" analysts*** to work in concert with analysts across the Community—to help fill gaps in strategic research as distinct from current reporting, to prompt collaboration on tasks that merit a Community perspective, and to help spread sound analytic methods and standards; and
- ***Daily intelligence support to the President***, without which the DNI would find it very hard to impose standards and priorities on organizations free to plead the exigencies of meeting immediate needs of important clients.

MANAGING THE COMMUNITY OF ANALYSTS

As we have discussed in our chapters on management and on collection, no single individual or office in today's Intelligence Community is responsible for getting the answers right on the most pressing intelligence issues of our day. We have recommended the creation of Mission Managers to fill this role, and they will perform a variety of essential tasks—including leading the development and management of collection strategies against high-priority intelligence targets. Because we believe that analysis must drive the collection process, it will be vital that Mission Managers also act as leaders in the analytic community. First and foremost, they must assess the strengths and weaknesses of analytic production in their areas of substantive responsibility.

These assessments will enable Mission Managers to develop strategic analysis plans to guide the Community's analytic efforts over the long term. Moreover, the assessments will guide Mission Managers in their role as chairs of Target Development Boards; their understanding of the gaps in analysts' knowledge will ensure that these gaps do in fact drive collection.

Armed with a clear understanding of where expertise resides in the Community, Mission Managers will also be able to foster competitive analysis. We expect that Mission Managers will ensure that finished intelligence routinely reflects the knowledge and competing views of analysts from all agencies in the Community. In particular, we expect that Mission Managers will encourage analysts to make differences in judgments, and the substantive bases for these differences, explicit in all finished products.

Recommendation 1

Mission Managers should be the DNI's designees for ensuring that the analytic community adequately addresses key intelligence needs on high priority topics.

To accomplish this, Mission Managers must have a comprehensive view of the skills and knowledge of the Community as a whole. The DNI should call on all agencies to provide—and regularly update—information about the knowledge and skills of their analysts, including their academic backgrounds, professional experiences, military experiences, and languages. The DNI's staff should make this information accessible through an easy-to-use directory and search tool. Mission Managers and agency heads would draw on this information to identify existing gaps, develop strategies to fill them, and create long-run strategic plans to avoid gaps on critical intelligence issues.

The model we envision is in stark contrast to the status quo, in which decisionmakers and analysts have little ability to find, track, and allocate analytic expertise. Although some efforts have been made to create such a database, ironically organizations have contributed information on the condition that other agencies not have access to their data. Our interactions with various agencies strongly suggest that the Intelligence Community still lacks a full understanding of the number, type, and skill-level of analysts in the various analytic organizations.[3] Therefore it is difficult to identify the

gaps in expertise for purposes of hiring, training, supervising professional development, or managing day-to-day work. Today, line managers identify the gaps in expertise in their own analytic organizations, but little is done to understand gaps from the perspective of an entire agency, much less the entire Community. With so weak a grasp of the Community's analytic resources, it is no wonder that agencies have difficulty quickly aligning their resources to respond to crises.

Even in the area of counterterrorism, which has consistently received high-level attention, agencies have struggled to establish a true Community analytic counterterrorism effort. The only way the Intelligence Community could bring together counterterrorism analytic expertise was to pull analysts away from their home agencies and house them together. From its inception, the Terrorist Threat Integration Center (now NCTC) faced fierce bureaucratic resistance in its efforts to do just this.

We believe a Mission Manager could respond to this or similar challenges more intelligently, quickly, and decisively. A Mission Manager would be able to (1) identify where analytic expertise resided and call on analysts from a variety of agencies to respond to critical questions; (2) identify and recommend to the DNI which analysts should be moved within or between agencies, if required in order to respond to a crisis; (3) "surge" on such a crisis, in the event that Community resources were insufficient, by tapping outside experts to contribute their expertise; (4) create a "virtual center" without physically co-locating analysts and without establishing a segregated and centrally-managed body to analyze a particular subject matter; and (5) clearly define organizational roles rather than letting bureaucratic dogfights, such as those surrounding TTIC, determine who has responsibility for which task. This, we believe, is how the analytical community should be managed.

Although Mission Managers would manage analysis by substantive area, they would not—in contrast to a center like the National Counterterrorism Center or the National Intelligence Council—actually *do* extensive intelligence analysis. Rather, a Mission Manager should coordinate and oversee decentralized analysis. By maintaining this separation of responsibilities, we believe that Mission Managers can prevent so-called "groupthink" among analysts. Indeed, we think fostering competitive analysis within the Community is a critical aspect of the Mission Manager's role.

We acknowledge that the Mission Managers will, if effective, interfere with the current autonomous management of analytic resources within individual organizations. But we see this as a strength, ensuring that members of the Community work together instead of at odds with one another. The risk, of course, is that a Mission Manager with a strong analytic viewpoint could reduce, rather than foster, competitive analysis. While this may sometimes happen—because Mission Managers must have substantive expertise to guide the Community's work—we expect Mission Managers to act more as facilitators of analytic products than as senior analysts. Consequently, their role most often should be to clearly present analytic viewpoints—including alternative views—to policymakers. If a Mission Manager fundamentally disagrees with the prevailing view in the Community, the Mission Manager could present his own view as an alternative, but he should not silence the perspective of other specialists in the Community.

Although not a precondition for success, our vision for Mission Managers ultimately requires a significant technological change—the creation of a "common work environment" for the community of analysts working on a topic. By "common work environment" we mean a shared information network with compatible computer tools and a common computer filing system for analytic products. Such technology is necessary to permit the Mission Manager to have full visibility into the emerging analytic work that is (or is not) being done on a topic, the basis for analytic assessments, and the degree of collaborative involvement between analysts and collectors. This common work environment will also enable greater collaboration between analysts in different agencies, as well as with the nucleus of analysts we recommend placing in the National Intelligence Council (see below).

A final note about managing the Intelligence Community's analysts: we recommend that one of the DNI's earliest undertakings be to have a senior advisor assess the Intelligence Community's medium- and long-term analytic needs, identify analytic gaps, and recommend ways to fill those gaps. And because the Intelligence Community's needs should be closely correlated with policymaker priorities, policymakers should be included in this assessment. Recommendations for correcting deficiencies might include such methods as targeted hiring, correcting national educational shortcomings, or contracting with outside experts.

TAPPING NON-TRADITIONAL SOURCES OF INFORMATION

Analysts have large quantities of information from a wide variety of sources delivered to their desktops each day. Given the time constraints analysts face, it is understandable that their daily work focuses on using what's readily available—usually classified material. Clandestine sources, however, constitute only a tiny sliver of the information available on many topics of interest to the Intelligence Community. Other sources, such as traditional media, the Internet, and individuals in academia, nongovernmental organizations, and business, offer vast intelligence possibilities. Regrettably, all too frequently these "nonsecret" sources are undervalued and underused by the Intelligence Community. To be true all-source analysts, however, Community analysts must broaden their information horizons. We encourage analysts to expand their use of open source materials, outside experts, and new and emerging technologies.

To facilitate analysts' productive use of open source information, the Intelligence Community should create an organization responsible for the collection of open source information. We discuss the need for an open source organization in greater detail in Chapter Seven (Collection). It merits emphasis here, however, that simply creating this organization is unlikely to be sufficient. Analysts who routinely receive clandestine reporting too often see unclassified reporting as less important, and they spend too little time reviewing and integrating data available through open sources. Analysts on lower priority accounts use open source materials because they have difficulty getting clandestine collectors to assist them, but even they receive little or no training on how to evaluate available open sources or find the best information most efficiently.

Recommendation 2

The DNI should create a small cadre of all-source analysts—perhaps 50—who would be experts in finding and using unclassified, open source information.

As the CIA increases its analytic workforce, a small number could be reserved and trained specifically in open source research. They could then be assigned to offices willing to experiment with greater use of open source

material, where they would be expected to answer questions for and provide useful unclassified information to analysts. They would also produce their own pieces highlighting open source reporting but drawing on classified information as well.[4] We see these "evange-analysts" as essentially leading by example. They should show other analysts how to find and procure useful open source material, how to assess its reliability and biases, and how to use it to complement clandestine reporting.

We acknowledge that, given the demand for more analysts, there are real costs to designating even this small number as open source specialists. But we expect that the need for these specialized analysts will not be permanent. Over time, the knowledge this group has about open sources is likely to be absorbed by the general population of analysts—as a result both of their education outreach efforts and of the influx of younger, more technologically savvy analysts. As this happens, these open source specialists can be absorbed into the broader analytic corps.

In addition to this special cadre of analysts, the Community will need to find new ways to deal with the challenges presented by the growing availability of open source materials. Among these challenges is the critical problem of processing increasing numbers of foreign language documents.

Recommendation 3

The DNI should establish a program office within the CIA's Open Source Directorate to acquire, or develop when necessary, information technologies to permit prioritization and exploitation of large volumes of textual data without the need for prior human translation or transcription.

Information technology has made remarkable advances in recent years. The private sector (without the same kinds of security concerns as the Intelligence Community) has led the adoption of technologies that are also critical to intelligence. Two areas show particular promise: first, machine translation of foreign languages; and second, tools designed to prioritize documents in their native language without the need for translation.

The Community will never be able to hire enough linguists to meet its needs. It is difficult for the Community to predict which languages will be most in

demand and to hire the necessary linguists in advance. And even an aggressive hiring and training effort would not produce an analytic workforce that can absorb the huge quantity of unclassified foreign language material available today.

Eventually, all analysts should have basic foreign-language processing tools easily available to them so that even those who are not language-qualified can pull pieces of interest and get a quick, rough translation. NSA has done pioneering work on machine translation and is pursuing a number of separate initiatives; the military services, CIA (including In-Q-Tel), and other agencies sponsor largely independent projects. There is an abundance of activity, but not a concerted, coherent effort, which has led to steady but slow development.

Advanced search and knowledge extraction technologies could prove to be even more valuable than machine translation (and of course, the two are very much related). We refer here to software that uses mathematical operations, statistical computations, and relational analyses to cluster documents and other data by subject, emphasis, and association in order to identify documents that are similar even when the documents do not use the same key words. Other types of software algorithms can discern concepts within a text; some can depict relationships between ideas or between factual statements based on an understanding of the word's meaning rather than merely searching for a word verbatim. As these tools mature, they will be invaluable to agencies that now find themselves collecting more information than they can analyze. They will also become essential to analysts caught in a similar avalanche of data.

The Intelligence Community has only begun to explore and exploit the power of these emerging technologies. The Intelligence Community's current efforts should be coordinated, consolidated where appropriate, directed, and augmented. Therefore, we suggest that the DNI establish a program office that can lead the Community effort to obtain advanced information technology for purposes of machine translation, advanced search, knowledge extraction, and similar automated support to analysis. This office would draw on the various initiatives in these areas dispersed throughout the Intelligence Community. It would work to avoid duplication of effort and would promote collaboration and cross-pollination. It would serve as a knowledge bank of state-of-the-art technology. It would also serve as a testbed, using open source information to

experiment with software that has not yet been certified for classified environments. When appropriate, it would hand off successful technologies for use on classified networks. While we would place the program office in the new Open Source Directorate, where quick deployment seems most likely to occur, we recognize that NSA is a center of excellence for linguistics and technology, and it must surf a data avalanche every day. For that reason, we suggest that the program office be jointly staffed by NSA and CIA.

Context Is Critical

Many of the intelligence challenges of today and tomorrow will, like terrorism or proliferation, be transnational and driven by non-state actors. Analysts who cover these issues will need to know far more than the inclinations of a handful of senior government officials; they will need a deep understanding of the trends and shifts in local political views, cultural norms, and economic demands. For example, analysts seeking to identify geographic areas likely to be receptive to messages of violence toward the United States will need to be able to distinguish such areas from those that, while espousing anti-U.S. rhetoric or advocating policies at odds with the interests of the United States, nevertheless eschew violent tactics.

Clandestine collectors, however, are poorly structured to fill the intelligence gaps these analysts face. Imagery is of little utility, and both signals and human intelligence are better positioned to provide insight into the plans and intentions of a few important individuals rather than broader political and societal trends.

As a result, analysts are supplementing clandestine collection not only with a greater reliance on open source material and outside experts, but also with their own expertise. To enable them to do so, the Intelligence Community must expand analysts' opportunities to travel and live overseas. And it must consider reforms to the security clearance process that often hampers recruitment of those with the most experience living and working among groups of interest to the Community. Failure to think creatively about how to develop an analytic cadre with a deep understanding of cultures very different from our own will seriously undermine the Community's ability to respond to the new and different intelligence challenges of the 21st century.

Recommendation 4

The Intelligence Community should expand its contacts with those outside the realm of intelligence by creating at least one not-for-profit "sponsored research institute."

We envision the establishment of at least one not-for-profit "sponsored research institute" to serve as a critical window into outside expertise for the Intelligence Community. This sponsored research institute would be funded by the Intelligence Community, but would be largely independent of Community management. The institute would both conduct its own research as well as reach out to specialists, including academics and technical experts, business and industry leaders, and representatives from the nonprofit sector and from Federally Funded Research and Development Centers.

Free from the demands created by the events of the day that burden those within the Intelligence Community, this sponsored research institute's primary purpose would be to focus on strategic issues. It would also serve as an avenue for a robust, external alternative analysis program. Whatever alternative analysis the Community undertakes internally—and we see this as essential—there must be outside thinking to challenge conventional wisdom, and this institute would provide both the distance from and the link to the Intelligence Community to provide a useful counterpoint to accepted views. In this vein, the DNI might consider establishing more than one such institute. By doing so, competitive analysis would be further promoted and healthy competition between the research institutes would help both from being co-opted by the Intelligence Community.

This sponsored research institute would eliminate some existing impediments to more extensive outreach. The institute would have a budget that would enable it to pay top experts unwilling to work for the lower rates typically offered by Intelligence Community components. Moreover, contractors linked to the institute would be available to all Intelligence Community components, avoiding any suggestion that contractors were tasked to provide assessments to support the views of a particular agency. Further, although the staff of the research institute would take recommendations from analysts for particular people to contact outside of the Community, we expect the staff itself to pull together possible contacts in critical fields, expanding the circle

of those whose knowledge would be available to the Intelligence Community. The sponsored research institute could also become a center for funding non-traditional methods of assembling open source information. In our classified report we provide an example that cannot be discussed in an unclassified format.

Such a sponsored research institute is not the only way to capitalize on expertise from outside the Intelligence Community. Although the institute would expand the Community's ongoing outreach efforts, the Intelligence Community also needs to think more creatively and, above all, more *strategically* about how it taps into external sources of knowledge. This may include recognizing that the Community may simply not be the natural home for real expertise on certain topics. While economic analysts, for example, can and do play a valuable role in the Community, economists at the Federal Reserve, World Bank, or private sector companies investing millions in emerging markets are likely to have a better handle on current market conditions. Relying on these experts might free up Community resources to work more intensely on finding answers no one else has.

Each of these proposals assumes the Community will have access to existing experts, but that will not always be the case. As a result, the Community must also find ways to support the development of the external expertise it needs. One biosecurity expert remarked that what we really need is a major effort to foster publicly-minded experts to tackle the biothreats likely to face the United States in the future.[5] Title VI of the Higher Education Act, which supports language and area studies in universities, and the National Security Education Program (the Boren Program) might also help. We believe the Intelligence Community should think even more broadly about ways to meet national information needs.

Finally, analysts also need to take full advantage of currently available and underutilized non-traditional technical intelligence capabilities, like advanced geospatial intelligence techniques and measurement and signature intelligence (MASINT). Analysts would benefit from additional training and education to increase their awareness of new and developing collection techniques, so that they are able to effectively task these sources and use the information provided.

MANAGING THE INFLUX OF INFORMATION

As countless groups both inside and outside the Intelligence Community have commented, there is a dire need for greater information sharing—or, as we prefer to put it, information *access* in the Intelligence Community. We address this topic more fully in Chapter Nine (Information Sharing).

But analysts not only need more information, they also need new ways to manage what is already available to them. Analysts today "are inundated and overloaded with information."[6] A study published in 1994 revealed that analysts on average had to scan 200 to 300 documents in two hours each day, just to discover reports worth writing about.[7] If we assume that relevant information has doubled for most analytic accounts over the past ten years (a gross understatement if open source information is considered)—and if we depend on analysts not just to pick reports to write about but instead to "connect the dots" among names, phone numbers, organizations, and events found in other documents—the typical analyst would need a full workday just to perform the basic function of monitoring new data.

The private sector is already using tools and techniques to handle the greatly increased flow of information in today's world; many of the best of these operate even before a user begins to look for relevant information. By the time an Internet user types search terms into Google, for example, the search engine has already done a huge portion of the work of indexing the information and sorting it by relevance. In fact, Google already has educated guesses about what information will be most useful regardless of the breadth of the user's search.

The Intelligence Community's widely used tools for processing raw intelligence traffic are far weaker. According to a senior official at CIA's In-Q-Tel, when analysts enter the Intelligence Community they discover that they have "left a world that was totally wired."[8] Today, an analyst looking for information on Intelligence Community computers is effectively performing a keyword search without any relevance ranking or additional context. The Community has been largely resistant to efforts to import tools from the private sector that offer new and different ways of using technology to exploit data.[9] While this resistance is often driven by legitimate concerns about security, these concerns can (and must) be overcome in the development of information technology for the Intelligence Community.

Recommendation 5

The Community must develop and integrate into regular use new tools that can assist analysts in filtering and correlating the vast quantities of information that threaten to overwhelm the analytic process. Moreover, data from all sources of information should be processed and correlated Community-wide *before* being conveyed to analysts.

The Intelligence Community is only in the beginning stages of developing effective selection, filtering, and correlation tools for its analysts, and more progress must be made. While in every case people are needed to see whether the proposed connections are real—and to be alert for intuitive but inchoate linkages—the Intelligence Community must more effectively employ technology to help draw attention to connections analysts might otherwise miss.

But better tools are not the whole answer. Time and again, tools introduced to the Intelligence Community have failed to take hold because the Community's analysts were accustomed to doing business a different way. We therefore believe there is a need to improve on the Community's long standing, but now outdated, basic approach to processing, exploiting, and disseminating information. In our view, the Intelligence Community needs processes that help analysts correlate and search large volumes of data after traditional dissemination by collectors but *before* the information overflows analysts' inboxes.

Without such a change, we are afraid that analysts will be overwhelmed by piles of information through which they have little hope of sorting.

FOSTERING LONG-TERM RESEARCH AND STRATEGIC THINKING

Managers and analysts throughout the Intelligence Community have repeatedly expressed frustration with their inability to carve out time for long-term research and thinking. This problem is reinforced by the current system of incentives for analysts, in which analysts are often rewarded for the number of pieces they produce, rather than the substantive depth or quality of their production.

Analysts are consistently pressed to produce more pieces faster, particularly those for current intelligence publications such as the President's Daily Brief (PDB). One analyst told us that if an office doesn't produce for the PDB, its "cupboard is bare."[10] But constant pressure to write makes it hard for analysts to find time to do the research—and thinking—necessary to build the real expertise that underlies effective analysis. In one particularly alarming example, an Iraq analyst related that the demand for current intelligence became so acute that he not only gave up long-term research, but also stopped reading his daily in-box of intelligence reporting. That task was delegated to a junior analyst with no expertise on Iraq weapons of mass destruction issues who pulled traffic he thought might be of interest.[11] Although this is an unusually dramatic example, we provide additional classified statistics illustrating this problem in our classified report.

The drive to fill current publications can also crowd out work on strategic military and proliferation issues. As with long-term research, work on these issues may fall by the wayside as analysts respond to immediate, tactical policymaker interests. And strategic work may be discouraged simply because presenting it in a format usable by current intelligence publications is difficult or impossible. Technical assessments are generally seen as too cumbersome for daily intelligence and more difficult for the non-technical briefers to discuss should the President choose to have a dialogue on the issue. Although some of these products reach senior policymakers separately, the fact that they are typically excluded from the publication designed to inform the President about the most important issues of the day likely suggests to analysts that this work is not as highly valued as other topics.

Managers with whom we spoke are aware of the dearth of strategic, long-term thinking, and are seeking ways to remedy the problem. However, we think that part of the solution lies within the new office of the DNI.

Recommendation 6

A new long-term research and analysis unit, under the mantle of the National Intelligence Council, should wall off all-source analysts from the press of daily demands and serve as the lead organization for interagency projects involving in-depth analysis.

We recommend placing this new unit under the National Intelligence Council where analysts would be able to focus on long-term research and underserved strategic threats, away from the demands of current intelligence production. Although some analysts in this new organization would be permanently assigned, at least half—and perhaps a majority—would serve only temporarily and would come from all intelligence agencies, including those with more specialized analysts, such as NGA and NSA. Typically, analysts would have two-year assignments in the unit; in some cases, analysts may spend shorter periods in the organization, long enough to complete a single in-depth research project of pressing need. Because we expect the topics tackled by this group to be complex, collaboration with those outside the unit should be pervasive.

We envision the analysts located in this unit leading projects that bring in experts from across the Intelligence Community, as well as from outside the sphere of intelligence. This collaboration will enable the Intelligence Community to tackle broad strategic questions that sometimes get missed as many analysts focus on narrow slivers of larger issues. DIA analysts and managers, for example, told us that the current division of key analytical responsibilities among the various Department of Defense intelligence units at DIA, the service intelligence centers, and the unified commands makes it difficult for DIA to develop an integrated, strategic assessment of emerging security issues. We expect this new organization to fill such gaps.

Some might be concerned that this new analytic unit would create unhealthy barriers between those engaged in current intelligence and those conducting long-term research. But as proposed, this office avoids that division. Using the common technology infrastructure we propose, we expect that analysts in the new office would easily be able to draw on the insight of analysts still in their home offices who are working on current intelligence. Moreover, because analysts would rotate through this office and remain only for a short period of time, they would not run the risk of veering off into studying questions that might be intellectually interesting but are unlikely to be important to decision-makers. These analysts would come to the office with an understanding of the pulse of current intelligence. Even more important, those same analysts would return to their line units, and the production of timely intelligence, with a greater depth of understanding of their accounts.

Rotations to this unit would also reinforce habits that should be second nature, but sometimes get lost in the daily press of business. Analysts would have time to think more carefully about their words, ensuring that terms used to express uncertainty or concerns about credibility were consistent over time and across accounts. We hope that this unit would also engage in alternative analysis—and that this would help to foster alternative analysis throughout the Intelligence Community. Moreover, rotations through this unit would foster a greater sense of community among analysts and spur collaboration on other projects as well.

Although this strategic analytic unit could be housed in a number of places, we believe that the NIC is best. First, the NIC remains today one of the few places within the Intelligence Community that focuses primarily on long-term, strategic thinking. Second, the NIC is already accustomed to working with analysts across the Community and is therefore likely to be seen as an honest broker—an organization that treats analysts from different agencies equally. Third, the NIC already regularly engages outside experts. Indeed, many National Intelligence Officers spend the bulk of their careers outside the intelligence field.

ENCOURAGING DIVERSE AND INDEPENDENT ANALYSIS

Throughout our case studies we observed the importance of analysts clearly identifying and stating the basis for their assessments. But good analysis goes well beyond just saying what is known, what is unknown, and what an analyst thinks. It is critical that analysts find ways of routinely challenging their initial assumptions and questioning their conclusions—in short, of engaging in competitive (or, as we prefer to call it, independent) analysis.

Recommendation 7

The DNI should encourage diverse and independent analysis throughout the Intelligence Community by encouraging alternative hypothesis generation as part of the analytic process and by forming offices dedicated to independent analysis.

We believe that diverse and independent analysis should come from many sources. In this vein we offer several recommendations that should foster diverse and independent analysis, most particularly our proposed long-term research and analysis unit in the National Intelligence Council, our proposed not-for-profit sponsored research institute, the preservation of dispersed analytic resources, and Community training that instills the importance of independent analysis.

To begin, we note ongoing efforts within the Intelligence Community that have provided valuable independent analysis. The CIA's Directorate of Intelligence, for example, currently has an organization that exclusively drafts "red cell" pieces—documents that are speculative in nature and sometimes take a position at odds with the conventional wisdom.[12] This office proved especially valuable in the context of Libya, for reasons we discuss in greater detail in our classified report but cannot discuss here.

We foresee our proposed long-term research and analysis unit augmenting such existing efforts. We envision the office conducting some of its own alternative analysis, working with analysts in their home offices to conduct independent analysis, and ensuring that analytic judgments are routinely challenged as new information becomes available. By both engaging in its own work and working in conjunction with other offices, we hope that the unit will help catalyze independent analysis throughout the Community and, in the long run, ensure that independent analysis becomes part of the standard way of thinking for all analysts.

Our envisioned not-for-profit sponsored research institute is another natural location for independent analysis to be conducted. In fact, a well-designed research institute should be ideal in that it would have close relationships with non-Intelligence Community experts, as well as easy access to large volumes of open source material. Similarly, the National Intelligence Council should further foster alternative analysis through a National Intelligence Estimate (NIE) process that promotes dissenting views. In our view, the NIE process today is designed to serve as a Community product and, as such, can sometimes become a consensus building process. We hope that the DNI will encourage the NIE drafters to highlight and explore dissenting opinions.

We must stress, however, the importance of fostering a culture of alternative analysis *throughout* the Intelligence Community, as opposed to centralizing

the function in a single office (or even several offices). An office solely responsible for dissenting opinions is at risk of losing credibility over time, which would not make it an attractive place for analysts to work. Moreover, we are afraid that an office dedicated to independent analysis would—in the long run—end up having its own biases, and would not provide the diversity of views that we think is so important.

We thus recommend that the DNI give particular "red-team" or "devil's advocate" assignments to individuals or offices on a case-by-case basis, rather than trying to produce all alternative analysis through a separate office. By doing so, no individual or office would constantly bear the brunt of criticizing other analysts' work, nor would such alternative analysis be thought to be the sole responsibility of a single, stand-alone office. And while the DNI is statutorily required to assign an individual or entity responsibility for ensuring that the Community engages in alternative analysis,[13] this should not in our view artificially limit the locations in which such analysis occurs.

Perhaps most important, however, is the view that the Intelligence Community should not rely upon specialized "red team offices," or even individual "red team exercises" to ensure there is sufficient independent analysis. Rather, such independent analysis must become a habitual analytic practice for *all* analysts. The decentralization of the Intelligence Community's analytic bodies will naturally contribute to independent and divergent analysis, and we believe that the Mission Managers we propose will play a valuable role in identifying and encouraging independent analysis in their topic areas. But the Intelligence Community must also ensure that analysts across the Community are trained to question their assumptions and make their arguments explicit. Alternative analysis should be taught in the very first analyst training courses as a core element of good analytic tradecraft. It is to this topic—the training of analysts—that we next turn.

IMPROVING TRADECRAFT THROUGH TRAINING

A common theme from our case studies is that the fundamental logical and analytic principles that should be utilized in building intelligence assessments are often inadequately applied. There are several reasons for this. Key among these is a leadership failure; managers of analysts have neglected to demand the highest standards of analytic craft. This management weakness has been compounded in recent years by the lack of experience among analysts, caused

by the more than 33 percent decline in the number of analysts from the latter part of the 1980s through most of the 1990s. On top of the numerical reduction, many of the *best* analysts left during this period because they were the ones who could easily get jobs outside of government. The outflow of knowledge was even greater than the outflow of people.

The Intelligence Community started slowly to hire more analysts in the late 1990s, and recent congressional and executive branch actions are now resulting in further expansion of the analytic corps. As a result, the Intelligence Community is now populated with many junior analysts and few mentors. And the focus on current intelligence has meant that few analysts are given the time to develop expertise, while managers have little time to develop management and mentoring skills.

These difficulties have reduced the quality of finished intelligence. When we reviewed finished intelligence, we found egregious examples of poor tradecraft, such as using a piece of evidence to support an argument when the same piece also supported exactly the opposite argument—and failing to note this fact. In some cases, analysts also failed to update or correct previously published pieces, which led other analysts and policymakers to make judgments on faulty or incomplete premises.

But far and away the most damaging tradecraft weakness we observed was the failure of analysts to conclude—when appropriate—that there was not enough information available to make a defensible judgment.[14] As much as they hate to do it, analysts must be comfortable facing up to uncertainty and being explicit about it in their assessments. Thankfully, we have found several instances of recent efforts by individual analysts to clearly admit what they do and do not know. In particular, a recent National Intelligence Estimate used new processes to ensure that source information was carefully checked for accuracy before inclusion in the estimate. In addition, the Estimate clearly highlighted the intelligence collection gaps on the topic and analysts' level of confidence in their judgments. In our classified report we discuss the particulars of this Estimate in greater depth. Still, these efforts have not been institutionalized, nor are they widespread. We heard many times from users of intelligence that they would like analysts to tell them up front what they don't know—something that intelligence analysts apparently do too infrequently.

Recommendation 8

The Intelligence Community must develop a Community program for training analysts, and both analysts and managers must prioritize this career-long training.

The Intelligence Community must reverse the erosion of analytic expertise that has occurred over the last 15 years. Analytic reasoning must be more rigorous and be explained in clearer terms in order to improve both the quality and credibility of intelligence. Specifically, analysts should take pains to write clearly, articulate assumptions, consistently use caveats, and apply standard approaches to sourcing. A renewed focus on traditional tradecraft methods needs to be augmented with innovative methodologies and tools that assist the analyst without inhibiting creativity, intuition, and curiosity.

This strengthening of the analytic workforce can only occur through a dedicated effort by the Intelligence Community to train analysts throughout their careers. A structured Community program must be developed to teach rigorous tradecraft and to inculcate common standards for analysis so that, for instance, it means the same thing when two agencies say they assess something "with a high degree of certainty." Equally important, managers and analysts must be held accountable for ensuring that analysts continue to develop expertise throughout their careers. The excuse, "I didn't have time for training," is simply unacceptable. This responsibility of both managers and analysts for continued tradecraft training should be made part of all performance evaluations.

Another critical element of training for analysts, and one that has been long lacking in the Intelligence Community, concerns their understanding of intelligence *collection*. Today, analysts receive too little training on collection capabilities and processes, and the training they do receive does not adequately use practical exercises to help analysts learn how to build effective collection strategies to solve intelligence problems. This fundamental ignorance of collection processes and principles can lead to serious misjudgments, and we recommend that the Intelligence Community strengthen analyst training in this area. In our classified report we point to areas in other intelligence agencies' training programs that we believe could be improved, but that cannot be discussed in an unclassified report.

What Denial and Deception (D&D) Means for Analysis

State and non-state actors either with or seeking to develop WMD materials and technologies all practice robust denial and deception techniques against U.S. technical collection. We must significantly reduce our vulnerability to intelligence surprises, mistakes, and omissions caused by the effects of denial and deception (D&D) on collection and analysis. To do so, the Community must foster:

- ***Greater awareness of D&D among analysts,*** including a deeper understanding of what other countries know about our intelligence capabilities, as well as the D&D intentions, capabilities, and programs of those countries.
- ***Greater specification by analysts of what they don't know and clearer statements of their degree of certainty.*** Analysts should also work more closely with collectors to fully exploit untapped collection opportunities against D&D targets, and to identify and isolate any deceptive information.
- ***Greater appreciation for the capabilities and limitations of U.S. collection systems.***
- ***Greater use of analytical techniques that identify the impact of denial and the potential for deception.*** Analysts must understand and evaluate the effects of false, misleading, or even true information that intelligence targets may have injected into the collection stream to deceive the United States.

Recommendation 9

The Intelligence Community must develop a Community program for training managers, both when they first assume managerial positions and throughout their careers.

Managerial training must also be vastly expanded throughout the Intelligence Community. Although scattered training is available, the Intelligence Community currently has no systematic, serious, or sustained management training program, and none that readily allows for cross-agency training—even though management problems can be similar across agencies. CIA managers,

for example, receive a small portion of the training provided to their military counterparts.[15] And we are dismayed that some in the Intelligence Community resisted programs such as merit-based pay due to a mistrust of managers' ability to accurately and fairly measure performance.

Prospective managers should be given extensive management training before assuming their responsibilities, and current managers should be enrolled in refresher training courses on a regular basis. A well-trained management and leadership corps within the Intelligence Community is vital to the health of analysis (and collection), and the Community is currently suffering the consequences of its absence. To the degree that a few individuals at the CIA have already recognized this problem, and are designing programs to address it, we commend them.

Although we hesitate to prescribe any specific level of centralization for analytic and managerial training, we do suggest that some of the training be Community-wide, perhaps housed in our proposed National Intelligence University or done through an online education program.[16] We do so in full recognition that individual agencies may want to conduct their own training because their workforce requires specialized skills, and that some resist centralized training on the grounds that training should engender a strong affiliation among analysts for their particular agency.

Notwithstanding these objections, as discussed in our chapter on Management, we believe that the creation of the DNI provides a unique opportunity to reconsider implementing some elements of Community training. The benefits will be enormous: it will teach common tradecraft standards, standardize teaching and evaluation, foster a sense of Community among analysts, and, we hope, provide analysts with a wider range of training opportunities throughout their careers. It may also create economies of scale in training costs. For these reasons, we strongly encourage joint training whenever feasible.

MAKING ANALYSIS MORE TRANSPARENT

Training analysts and managers to use better "tradecraft" is only half the battle; rigorous analytic methods must be demanded in every intelligence product. One way of doing so—and at the same time ensuring that customers are confident in the intelligence they receive—is to make the analytic process

more transparent. Although we recognize that real security issues make total transparency impossible, we fear that protecting sources and methods has resulted in the shrouding of analysis itself, not just the intelligence on which it is based. This tendency must, we believe, be actively resisted.

Recommendation 10

Finished intelligence should include careful sourcing for all analytic assessments and conclusions, and these materials should—whenever possible in light of legitimate security concerns—be made easily available to intelligence customers.

We recommend forcing analysts to make their assumptions and reasoning more transparent by requiring that analysis be well sourced, and that all finished intelligence products, either in paper or in digital format, provide citations to enable user verification of particular statements. This requirement is no more rigorous than that which is required in law, science, and the social sciences, and we see little reason why such standards should not be demanded of the Intelligence Community's analysts. Analysts are generally already expected to provide sources for internal review; including this information in finished analysis would simply increase the transparency of the process.

We further recommend that customers have access to the raw intelligence reporting that supports analytic pieces whenever possible, subject to legitimate security considerations. For many intelligence customers, especially senior policymakers and operators, a general description, such as State Department "diplomatic reporting" simply does not provide the confidence needed to take quick and decisive action.[17] Where a user accesses finished intelligence electronically, he should be able to link directly to at least some portion of the raw intelligence—or to underlying finished intelligence—to which a judgment is sourced.

Requiring that citations be routinely available and linked to source documents need not preclude analysts from making judgments or inferences; rather, the availability of such materials will simply enable users to distinguish quickly between those statements that are paraphrased summaries of intelligence reporting, and those that are analytic judgments that draw inferences from this reporting. Of course, some analysts might worry that such a system would

essentially sideline the analyst, making his or her work irrelevant because all of his or her hard calls could be "questioned" by returning to the original sources and performing the analysis independently. We do not, however, think this is inherently bad. Intelligence customers should be able to question judgments, and analysts should be able to defend their reasoning. In the end, such a reform should bolster the stature of good analysts, as policymakers and operators come to see their analytic judgments as increasingly accurate and actionable.

Recommendation 11

The analytic community should create and store sourced copies of all analytic pieces to allow readers to locate and review the intelligence upon which analysis is based, and to allow for easy identification of analysis that is based on intelligence reports that are later modified.

We recommend that the DNI create a system to electronically store sourced versions of analytic pieces and ensure that source information is easily accessible to intelligence users, consistent with adequate security permissions. Of course, to make such electronic storage and accessibility possible one needs first to have a truly integrated information sharing environment and shared information technology systems—a considerable challenge given the inadequacies of today's information technology environment, on which we comment more fully in Chapter Nine (Information Sharing).

The DNI should also encourage the development of a system that enables Intelligence Community personnel to update intelligence information that has been judged to be unreliable, of increased or decreased certainty, or simply retracted. These updates must be electronically flagged in the intelligence reports themselves as well as any analytic products citing to the reports. Such tracking systems have existed in other fields for decades (*e.g.*, Lexis and Westlaw for the legal world).[18]

Above and beyond the technical constraints to implementing such a system, there are several barriers that have blocked these reforms in the past. For example, CIA's Directorate of Operations maintains a close hold on its highly sensitive reporting, often with good reason. Making this raw reporting accessible to policymakers and intelligence officers across the Commu-

nity raises several security and counterintelligence-related concerns. Furthermore, it is questionable to what degree *all* policymakers will need access to raw reporting.

But none of these issues explains why the Intelligence Community's efforts in this vein are still in such a stage of infancy. While there will be information that cannot be provided to intelligence customers, many decisionmakers can and do read intelligence reporting at the same time as the analysts who receive it. Further, access to an analytic product is typically limited to those who are cleared to read the intelligence reports on which it is based. The easy availability of source information, related reporting, and other finished intelligence products, along with a system to clearly identify old intelligence that has been reconsidered in one way or another, will benefit both analysts and customers. Analysts will, we believe, do their work more meticulously and accurately, while customers will be able to better understand the products they receive and know whether the Community continues to stand behind the intelligence.

IMPROVING SCIENTIFIC, TECHNICAL, AND WEAPONS INTELLIGENCE

Recommendation 12

The DNI should develop and implement strategies for improving the Intelligence Community's science and technology and weapons analysis capabilities.

A specific subset of analysts within the Intelligence Community is responsible for assessing emerging threats to U.S. interests resulting from advances in foreign science and technology (S&T) and weapons developments. Using specialized scientific and technical expertise, skills, and analytic methodologies, these analysts work on some of today's most important intelligence issues, including counterproliferation, homeland security, support to military operations, infrastructure protection, and arms control. We are therefore concerned that a recent Intelligence Science Board study concluded that the Intelligence Community's current S&T intelligence capability is "not what it could be and not what the nation needs."[19]

The Intelligence Science Board study and our own research found that the Intelligence Community's ability to conduct S&T and weapons analysis has

not kept pace with the changing security environment.[20] The board's study noted the Intelligence Community was particularly vulnerable to surprise by "rapidly changing and readily available emerging technologies whose use by state and non-state actors, in yet unanticipated ways, may result in serious and unexpected threats."[21] The S&T areas of most concern include biological attacks, nuclear threats, cyber warfare, Chinese technology leapfrogging, and the impact of commercial technologies on foreign threats.[22] In addition, current analysis often fails to place foreign S&T and weapons developments in the context of an adversary's plans, strategy, policies, and overall capabilities that would provide customers with a better understanding of the implications for U.S. security and policy interests.[23] One senior Administration official interviewed by the Commission staff described the Intelligence Community's capability to conduct this kind of all-source S&T and weapons analysis as "pretty poor" and "mediocre at best."[24]

The state of the Intelligence Community's S&T and weapons analysis capabilities should be a key issue for the DNI, given the importance of these fields in providing warning and assessments of many of today's critical threats. In addition to hiring more analysts with technical and scientific skills and experience, the Intelligence Community would benefit from more contact with outside technical experts who could conduct peer reviews and provide alternative perspectives. In addition, resources should be set aside for conducting in-depth and multidisciplinary research and analysis of emerging technologies and weapon developments to help the Community keep pace with the ever-changing security environment. The use of analytical methodologies, such as red teaming, scenario analyses, and crisis simulations, to explore and understand the impact of new technologies and weapons on U.S. interests should also be encouraged to help analysts guard against technology surprise.

To ensure progress will be made in the future, we recommend that the DNI designate a Community leader for developing and implementing strategies for improving the Intelligence Community's S&T and weapons analysis capabilities. This person should report to the DNI on a periodic basis on the status of the Community's relevant capabilities and make recommendations on where further improvements are needed.

SERVING INTELLIGENCE CUSTOMERS

Analysts are the link between customers and the Intelligence Community. They provide a conduit for providing intelligence to customers and for conveying the needs and interests of customers to collectors. This role requires analysts to perform a number of functions. Analysts must assess the available information and place it in context. They must clearly and concisely communicate the information they have, the information they need, the conclusions they draw from the data, and their doubts about the credibility of the information or the validity of their conclusions. They must understand the questions policymakers ask, those they are likely to ask, and those they should ask; the information needed to answer those questions; and the best mechanisms for finding that information. And as analysts are gaining unprecedented and critically important access to operations traffic, they must also become security gatekeepers, revealing enough about the sources for policymakers to evaluate their reporting and conclusions, but not enough to disclose tightly-held, source-identifying details.

Analysts fulfill these functions through interactions with a wide range of intelligence customers, who run the gamut in terms of rank, area of responsibility, and understanding of intelligence. "Typical" customers include not only the President and senior policymakers, but also members of Congress, military commanders, desk officers in executive agencies, law enforcement officers, customs and border patrol officials, and military units in the field. We do not attempt to examine each of these relationships, but we do note some challenges in this area. Specifically, we address how the Intelligence Community might modernize some customer relationships, some components of an "appropriate" relationship between analysts and customers, and how the President—and to a lesser degree other senior policymakers—should be supported.

Modernizing the Analyst-Customer Relationship

Recommendation 13

The DNI should explore ways to make finished intelligence available to customers in a way that enables them—*to the extent they desire*—to more easily find pieces of interest, link to related materials, and communicate with analysts.

The Intelligence Community must distribute its products more efficiently and effectively. Today's policymaker receives intelligence in almost the same way as his 1985 predecessor; most intelligence products from the CIA's Directorate of Intelligence, for example, are still delivered in hardcopy. For some customers, this may remain the preferred method of receiving intelligence. For others with different needs or preferences—and we have heard from some of them—the Intelligence Community should consider ways to modernize intelligence distribution.

Some modernization has occurred; most notably, a limited number of Washington policymakers can access some intelligence products through the Defense Department's secure networks—JWICS and Intelink—at their desk. But the "populating" of these networks varies across agencies and by product type. For example, INR and DIA routinely place their publications on these secure networks, and a large percentage of finished intelligence products related to counterterrorism can be found online. By contrast, CIA sharply limits the use of its finished intelligence on these networks, citing the need to protect its human sources. And even when intelligence is available on electronic networks, the interfaces are clumsy and counterintuitive—far below the presentation of online publishers such as the *Washington Post*.

This state of affairs is markedly inferior to the state of the practice in private industry. Most customers of intelligence products cannot search electronic libraries of information or catalogues of existing products. They cannot query analysts in real time about needed information or upcoming products. They cannot link finished intelligence documents together electronically to create a reference trail. They cannot easily review research programs to provide suggestions or recommendations. They cannot explore thoughts and views with analysts in an informal online environment. They cannot read informal mes-

sages alerting them to new information which may include analysts' preliminary thoughts or judgments on an item. They cannot tailor information displays to their needs. They cannot reshape raw data into graphics and charts. They cannot access different intelligence media electronically.

This is not an area in which there is only one right answer; there are many ways to provide up-to-the-minute, in-depth information to policymakers in user-friendly formats. We also recognize that because of the dramatic effects an electronic system would have on the way the Intelligence Community does its work and because of substantial security concerns, any new program along these lines will require a great deal of additional thought and planning. Nevertheless, we believe that even in the relatively near future the benefits of an integrated electronic system will outweigh the risks, and it will become more necessary as a new generation of customers—with a preference for the flexibility of digital technology—reaches higher levels of government.

Components of the Analyst-Customer Relationship

Regardless of how customers receive intelligence, both analysts and customers have to recognize that certain exchanges between the two are appropriate and should be encouraged. Perhaps most importantly, we believe it is critical that customers engage analysts. It is the job of the analyst to express clearly what the analyst knows, what the analyst doesn't know, what the analyst thinks, and why—but if the analyst does not, the customer must insist that the analyst do so. If necessary, the customer should challenge the analyst's assumptions and reasoning. Because they are "keepers of the facts," analysts can play a decisive role in policy debates, a role that has temptations for analysts with strong policy views of their own. A searching examination of the underlying evidence for the analysts' factual assertions is the best way to reassure policymakers that the analysts' assertions are well-grounded. We reject any contention that such engagement is in itself inappropriate or that the risk of "politicizing" intelligence cannot be overcome by clear statements to analysts as to the purpose of the dialogue. When an analyst leaves a policymaker's office feeling thoroughly cross-examined and challenged to support his premises, that is not politicization; it is the system working at its best. Only through active engagement of this sort will intelligence become as useful as it can be.

Analysts also have a responsibility to tell customers about important disagreements within the Intelligence Community. We were told by some senior policymakers that it sometimes took weeks to get an answer to a question—not because the answer was difficult to obtain, but because analysts were hesitant to admit to Intelligence Community disagreement on an issue. This is not how intelligence should function. Analysts must readily bring disagreement within the Community to policymakers' attention, and must be ready to explain the basis for the disagreement. Such disagreement is often a sign of robust independent analysis and should be encouraged.

In addition to conveying disagreements, analysts must also find ways to explain to policymakers degrees of certainty in their work. Some publications we have reviewed use numerical estimates of certainty, while others rely on phrases such as "probably" or "almost certainly." We strongly urge that such assessments of certainty be used routinely and consistently throughout the Community. Whatever device is used to signal the degree of certainty—mathematical percentages, graphic representations, or key phrases—all analysts in the Community should have a common understanding of what the indicators mean and how to use them.

Finally, analysts and Intelligence Community leaders have a responsibility to take note, whenever possible, of what their customers are doing and saying, and to tell those customers when actions or statements are inconsistent with existing intelligence. We do not mean to suggest that analysts should spend all of their waking hours monitoring policymakers, or that analysts should have a "veto" over policymaker statements. Rather, when aware of upcoming speeches or decisions, analysts should make clear that they are available to vet intelligence-related matters, and analysts should—when necessary—tell policymakers how their statements diverge from existing intelligence. Having fulfilled this duty, analysts must then let politically-accountable policymakers determine whether or not a statement is appropriate in light of intelligence judgments.

Serving the President and Senior Policymakers

The new legislation designates the DNI as the person primarily responsible for ensuring that the President's day-to-day intelligence needs are met.[25] This means that the Office of the DNI, not the Director of the Central Intelligence Agency, should have the final authority over the content and production of the

President's Daily Brief (PDB)—or whatever other form intelligence support to the President may take.

We also believe that the DNI will have to work closely with the President and the National Security Council to reconsider how intelligence should best be presented to the President, because we are dubious that the PDB—in its current incarnation—is the right answer.

Our case studies, primarily Iraq, highlight several flaws indicating a need to rethink the PDB.[26] PDB pieces are typically limited by space constraints. While sophisticated, in-depth analysis can be presented in this abbreviated fashion, the task is considerably more difficult than drafting a more immediate, less research-intensive piece that updates the reader on current events and provides a more limited, near-term analytic focus. As a result, we worry that individual PDB articles fail to provide sufficient context for the reader. This view was reinforced by one senior intelligence officer's observation that policymakers are sometimes surprised to find that longer, in-depth intelligence reporting provides a different view from that conveyed by the PDB. The same individual noted that when a policymaker is given a piece of information about a certain subject, the policymaker will often ask questions about the information, leading to follow-up on that subject, thereby exacerbating the current intelligence bias.[27] Moreover, the PDB staff tends to focus on today's hot national security issues, or on issues that attracted the President's interest the last time they came up. This can lead to repeated reporting on a given topic or event; a drumbeat of incremental "hot news" articles affects a reader much differently than the same information presented in a longer, contextualized piece that explains the relationship between the various reports. Finally, the PDB sometimes includes excessively "snappy" headlines, which tend to misrepresent an article's more nuanced conclusions, and which are, in our view, unnecessary; a two or three-word indicator of the piece's subject (such as "North Korea-Nuclear") would tell policymakers which pieces were of most interest to them without obscuring the subtle contours of an issue raised in the text.

Having identified these potential problems, we are hesitant to suggest how the PDB process should be altered. Only the President can say for certain how often and in what format he prefers to receive national intelligence information. We do, however, recognize that the creation of the DNI will shift what

has been a CIA-centric PDB process to more of a Community one—shepherded by the Office of the DNI.

Recommendation 14

The President's Daily Brief should be restructured. The DNI should oversee the process and ensure a fair representation of divergent views. Reporting on terrorism intelligence should be combined and coordinated by the DNI to eliminate redundancies and material that does not merit Presidential action.

Regardless of the structure of the PDB process, the DNI will need to respond to the demands of senior advisors and the President. We recommend that the DNI create an analytic staff too small to routinely undertake drafting itself, but large enough that its members would have expertise on a wide range of subjects. The staffers would task the appropriate experts and agencies to draft responses to decisionmaker requests. They could also perform last minute editing and would—in every case—ensure that the pieces reflect any differences of opinion in the Community.[28] In our view, it is simply not enough to present dissenting views from the Intelligence Community only in longer, more formal assessments like National Intelligence Estimates. Rather, because policymakers tend to be significantly influenced by daily intelligence products, we believe it is essential that those products offer as complete a perspective on an issue as is feasible. This is not to suggest that the production of each daily briefing for the President or others should recreate a mini-NIE process; in many cases, relatively few intelligence agencies need be involved. But when agencies have sharp differences, the DNI's analytic staff should be responsible for ensuring that the final memorandum clearly reflects these competing conclusions and the reasons for disagreement.

Equally important, we believe that the DNI should seek to combine—with the President's concurrence, of course—the three primary sources of intelligence that now reach the President. Currently, in addition to the PDB, the President receives the President's Terrorism Threat Report (PTTR), which is prepared by the National Counterterrorism Center and is appended to each day's PDB. The President may also be verbally briefed by the Director of the FBI who uses material from a "Director's Daily Report" prepared by his staff.

We have reviewed these materials and discussed the briefings with many regular participants. There are plainly redundancies that should be eliminated, but we are also concerned that the channels conveying terrorism intelligence are clogged with trivia. One reason for this unnecessary detail is that passing information "up the chain" provides bureaucratic cover against later accusations that the data was not taken seriously. As one official complained, this behavior is caused by bureaucracies that are "preparing for the next 9/11 Commission instead of preparing for the next 9/11." It may be difficult to stem this tide, but the new DNI is in the best position to bring order to the process. We recommend that the DNI be given clear responsibility for combining terrorism intelligence into a single, regular Presidential briefing (whether a daily briefing is required should depend on the pace of events). This briefing would resemble and would perhaps be combined into the PDB.

In the same vein, several senior officials told us that they read the PDB not so much for its content (for it often did not necessarily include especially critical information) as much as to stay apprised of matters on which the President is briefed. In this light, although the DNI and the PDB staff must be free to make a professional judgment about the intelligence to present on any given day, we recommend that the DNI encourage suggestions from policymaking agencies like State and Defense about topics that could usefully be presented in the President's briefing. By taking this step the PDB would likely become more attuned to a wider variety of pressing national security issues.

We fully recognize that the DNI's role calls for a delicate balance. It will be tempting for the DNI's analysts to become the primary drafters themselves, and analysts in individual agencies will continue to face demands from those in their chain of command to respond to requests directly. The former would turn the office of the DNI into one more analytic entity putting forward its own views. The latter problem recreates the situation we have today, which often results in a multiplicity of uncoordinated views appearing before senior decisionmakers. The DNI's analytic cadre, whose responsibility it is to understand and to put forward the views of the Community's experts, wherever located, must ensure that analytic differences in the Community are not suppressed and, equally important, are not presented to decisionmakers in a piecemeal fashion that forces senior officials to sort out the differences themselves.

RETAINING THE BEST ANALYSTS

The Intelligence Community is unlikely to have the funding necessary to rely exclusively—or even primarily—on economic incentives to recruit and retain the best and the brightest. The Community, however, has always offered analysts something more: the opportunity to play a role in shaping the decisions of the nation's top leaders and to help maintain the security of our nation. To the extent that the Community loses sight of this as a motivating factor for its employees, it loses its most valuable tool for recruitment and retention.

Recommendation 15

The Intelligence Community should expand the use of non-monetary incentives that remind analysts of the importance of their work and the value of their contributions to national security.

Recognize good performers. The Intelligence Community should look for ways to ensure that the best analysts are recognized both within the Community and by decisionmakers outside of the Community. The fact that the Community on the whole works in relative anonymity makes this recognition all the more necessary. Analysts who are viewed as experts get the opportunity to do exactly what analysts are hired to do—play a part in shaping U.S. policy. In turn, analysts who have the chance to sit face-to-face with top-level decisionmakers are motivated in a very personal way to do their best.

Provide travel, training, rotations, and sabbaticals. All analysts are not alike, and not all opportunities for professional development will appeal to all equally. But giving analysts time to do the things they most want to do, particularly when the activities also contribute to the development of their expertise, is beneficial to everyone. One DIA manager told us that fully funding a robust travel budget would be far cheaper than paying salaries on a par with those paid by contractors, and would help a great deal in keeping analysts motivated and interested.[29] Other analysts are likely to find other activities more appealing, from full-time academic training, to policy rotations, to stints in the Office of the DNI or other agencies within the Community.

Permit careers to focus on the analysts' areas of interest. Analysts also differ in their preferred approaches to their careers. Some enjoy being generalists,

moving among all types of accounts and bringing a fresh perspective; others have a strong interest in a certain type of analysis—such as conventional weapons—or an area of the world, and might choose to spend time on a variety of similar accounts. Still others seek to specialize on fairly focused subject matters. The Intelligence Community benefits from all of these career paths, and in the best of all worlds, analysts would be able to follow the one best suited to their interests. The nature of the intelligence business will never allow for such a perfect fit; some specialists will need to remain on an account after their interest in it has waned, and some analysts will be pulled from where they are happiest to respond to an emerging crisis. But the goal should be to get it right for as many analysts as possible. Doing so is an enormously powerful retention tool. Managers of technical analysts explained to us that they had a great deal of difficulty retaining analysts because they came in expecting to work on areas in which they had developed expertise, but were pulled by the demands of the job into other areas that they found less interesting.[30] We expect that the Mission Managers will be able to place more focused attention on long-range planning and generate an increased understanding of where knowledge and expertise reside—and thus better position the Community to respond to emerging crises in a thoughtful way and reduce the numbers of analysts forced into jobs they dislike.

Provide tools and support. Managers also complained that analysts often find that the tools and technology available in the Intelligence Community fall short of what they use in school, at home, or in the private sector.[31] Moreover, analysts across the board face declining administrative support. Among other things, analysts typically must do desktop publishing, maintain files of classified materials not available electronically, manage contracts, and perform logistical tasks associated with travel or training. In other words, analysts often view their counterparts in the private sector as having better tools and better support that enable them to spend their time and energy on core tasks. Giving analysts what they need to do their job and ensuring that they spend their time as *analysts*, not clerks or administrative aides, would emphasize that their time and skills are valued.

LEARNING FROM PAST MISTAKES

The new intelligence reform legislation requires the DNI to assign an individual or entity the responsibility to ensure that finished intelligence products are timely, objective, independent of political considerations, based on all sources

of available intelligence, and grounded in proper analytic tradecraft. In the course of conducting relevant reviews, this entity is further directed to produce a report of lessons learned.[32]

Recommendation 16

Examinations of finished intelligence should be routine and ongoing, and the lessons learned from the "post mortems" should be incorporated into the intelligence education and training program.

Iraq, Libya, and Afghanistan have offered opportunities for the Intelligence Community to compare its assessments with the ground truth and examine the sources of the disparities. We have already seen evidence that the lessons learned from Iraq are being incorporated by analysts covering other countries or intelligence topics. Analysts are increasingly careful to explain their analytical baseline in their products, and attribute the sources of intelligence underlying it. The Intelligence Community, analysts say, has adopted the "rule of elementary school math class," in that its analysts are dedicated to "showing our work" to prevent the "layering of analysis."[33]

This is an area in which the Intelligence Community should learn from the Department of Defense, which has an especially strong, institutionalized process for benefiting from lessons learned. In our classified report, we discuss a Defense Department "lessons-learned" study that we found particularly impressive, but that we cannot elaborate upon here. Intelligence Community lessons-learned efforts (such as CIA's Product Evaluation Staff) had less success, in part because they do not have sufficient resources or possess much prestige within intelligence agencies. Nor do we think that, in general, intelligence agencies should be responsible for "grading their own papers." The intelligence reform legislation recognizes the need for a separate body that conducts reviews of analysis, a welcome idea that should be fully embraced by the Community.

CONCLUSION

The changes that we recommend are significant departures from the current way in which the Community conducts the business of analysis. Some run counter to long-standing, embedded practices, and we are mindful that they

may be resisted by analysts and managers alike. We believe, however, that these changes are essential to improving the Community's capability to accurately assess threats and to provide timely, relevant, thoughtful support to policymakers. Intelligence analysis faces unprecedented challenges; unprecedented measures to strengthen the analytical process are well warranted.

ENDNOTES

[1] U.S. Senate, *The Final Report of the Select Committee To Study Governmental Operations with Respect to Intelligence Activities* (April 26, 1976) (*i.e.*, Church Committee Report); Permanent Select Committee on Intelligence, U.S. House of Representatives, *IC21: Intelligence Community in the 21st Century* (1996); Commission to Assess the Ballistic Missile Threat to the United States (*i.e.*, Rumsfeld Commission), *Side Letter to the President* (March 18, 1999); CIA, *The Jeremiah Report: The Intelligence Community's Performance on the Indian Nuclear Tests* (June 1, 1998); Markle Foundation Task Force, *Creating a Trusted Information Network for Homeland Security* (Dec. 2003); National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (*i.e.*, The 9/11 Commission Report) (2004); Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence: Report of an Independent Task Force* (1996); Commission on the Roles and Capabilities of the United States Intelligence Community (*i.e.*, Aspin-Brown Commission), *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (1996); *Report of the Commission on Organization of the Executive Branch of the Government* (*i.e.* Hoover Commission Report) (1949).

[2] Staff review of House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence Markups of Intelligence Authorization Bills, 1991-2005.

[3] Interview with senior intelligence official (Sept. 22, 2004).

[4] The CIA has had similar programs in the past whereby the agency introduced analysts who were tools experts to work alongside other analysts. These analysts were just like their analytic colleagues, except that they were also specialists in how to use analytic technologies and could help counterparts learn to use these tools to structure research problems. CIA Office of Research and Development, *Office of East Asian Analysis Testbed Project Final Report* (Sept. 30, 1994).

[5] Interview with biosecurity expert (Feb. 4, 2005).

[6] Inter-agency Information Sharing Working Group, *Consolidated Report* (Dec. 14, 2004) at p. 5. We provided an additional footnote illustrating the magnitude of this challenge in our classified report.

[7] CIA Office of Research and Development, *Office of East Asian Analysis Testbed Project Final Report* (Sept. 30, 1994).

[8] Interview with senior In-Q-Tel official (Feb. 3, 2005). In addition, a senior manager of analysis told us he knew there is a need to make better use of open sources but that this could not be achieved without assistance in the form of preliminary correlation of the data. Interview with senior CIA DI official (Feb. 10, 2005).

[9] Interview with senior In-Q-Tel official (Feb. 3, 2005).

[10] Interview with CIA analysts (Jan. 24, 2005).

[11] Interview with former CIA WINPAC analysts (Nov. 10, 2004).

[12] These formal alternative analysis programs are also reinforced by the existence of multiple analytic units in the Community, which often reach different analytic conclusions.

[13] The DNI is statutorily required to assign responsibility "for ensuring responsibility that, as appropriate, elements of the Intelligence Community conduct alternative analysis." Intelli-

gence Reform and Terrorism Prevention Act of 2004 at § 1017, Pub. L. No. 108-458 (hereinafter "IRTPA").

[14] Chapter Three (Afghanistan).

[15] Interview with senior CIA official.

[16] There currently exist several very successful joint training programs. The Joint Military Intelligence College, for example, currently operates a very successful program—a structured intermediate/advanced curriculum for Intelligence Community officers across the Community. At the same time, many similar efforts have failed for various reasons, including insufficient funding and lack of bureaucratic clout. The Defense Department Chancellor for Civilian Education's program is one such example of an unsuccessful cross-agency effort. Interview with former senior staff of the defunct Department of Defense Office of the Chancellor for Civilian Education and Development (Jan. 13, 2005).

[17] Some, but not most, of the finished intelligence provided to the Commission included lists of reference numbers identifying particular sources, but we understand that such lists are not routinely provided to policymakers. In any case, these lists provide no indication of how one could determine which specific document supported facts included in the piece.

[18] We recognize that the DCI is currently working to establish Community procedures for such a system, and we commend this development. Chapter One (Iraq) provides a detailed discussion of how analysts and intelligence users continued to use reporting considered unreliable.

[19] DCI Intelligence Science Board Task Force, *The State of Science and Technology Analysis in the Intelligence Community* (April 2004) at p. xiii (hereinafter "ISB Report").

[20] *Id.* at p. xiii; Interview with senior intelligence official (Oct. 7, 2004); Interview with senior DIA analyst (Sept. 23, 2004).

[21] ISB Report at pp. 26-27.

[22] *Id.* at p. 27.

[23] *Id.* at pp. 26, 28; Interview with administration official (Sept. 30, 2004); Interview with administration official (Sept. 10, 2004).

[24] Interview with senior administration official (Oct. 12, 2004).

[25] IRTPA at § 1011.

[26] In addition, several senior policymakers expressed concerns about the utility of the PDB in its current incarnation.

[27] Interview with senior intelligence analyst (Nov. 8, 2004).

[28] We understand that the CIA is already moving in this direction and we commend it for doing so.

[29] Interview with DIA analysts and managers (Oct. 26, 2004).

[30] *See, e.g.*, Interview with CIA WINPAC analysts (Oct. 14, 2004).

[31] *Id.*

[32] IRTPA at § 1019.

[33] Interview with DIA analysts (Nov. 22, 2004).

CHAPTER NINE
INFORMATION SHARING

Summary & Recommendations

While the imperative to improve information sharing within and beyond the Intelligence Community is widely acknowledged, it is too infrequently noted that the Intelligence Community—and the new DNI—have an additional responsibility that is often in tension with the first: the need to protect intelligence sources and methods. What therefore is needed—and what is largely absent from today's Intelligence Community—are structures and processes for sharing intelligence information that are driven by commonly accepted principles of *risk management*. While some collection agencies have greatly improved their information sharing practices since September 11, others have allowed overly stringent protective requirements to play too decisive a role in the decision whether to share information. Concern about security in a narrow sense should not crowd out actions to ensure national security in the larger sense. Sometimes—indeed, often—the right answer will be to limit access to information because of security concerns; but collection agencies, which for perfectly understandable bureaucratic reasons may systematically undervalue the need to share information, should not make this decision.

Accordingly, in this chapter we call for a consolidation of authority and the centralized management of intelligence information along the following lines:

- Resolve management ambiguities created by the recent intelligence reform legislation through two actions: (1) ensure that the newly-created Program Manager reports to the President through the DNI; and (2) expand the Information Sharing Environment envisioned by the statute to include all intelligence information, not just intelligence related to terrorism;
- Create a single position under the DNI with responsibility for both information sharing and the protection of sources and methods: a chief information management officer; and
- Break down both policy and technical barriers to information sharing by eliminating inconsistent agency practices and establishing, to the fullest extent possible, uniform standards across the Intelligence Community designed to facilitate implementation of a networked community.

An End to "Sharing"

We begin with an important reservation about terminology. The term information "sharing" suggests that the federal government entity that collects the information "owns" it and can decide whether or not to "share" it with others. This concept is deeply embedded in the Intelligence Community's culture. We reject it. Information collected by the Intelligence Community—or for that matter, any government agency—belongs to the U.S. government. Officials are fiduciaries who hold the information in trust for the nation. They do not have authority to withhold or distribute it except as such authority is delegated by the President or provided by law. As we have noted elsewhere, we think that the Director of National Intelligence could take an important, symbolic first step toward changing the Intelligence Community's culture by jettisoning the term "information sharing" itself—perhaps in favor of the term "information integration" or "information access." But as the term "information sharing" has become common parlance, we will use it in this chapter to avoid confusion.

INTRODUCTION: THE LAY OF THE LAND

The 9/11 Commission Report depicted a number of failures by one agency to pass terrorism warning information to other agencies, resulting in missed opportunities to apprehend terrorists.[1] Although the problem of information sharing was not a central part of the Intelligence Community's failure to assess Iraq's weapons programs properly, our study of Iraq found several situations where key information failed to reach those who needed it: for example, poor information systems resulted in a failure to recall reporting from a source who was determined to be a fabricator, and early reporting raising questions about the credibility of Curveball was not widely distributed to the analytical community.[2] Our review of other aspects of the Intelligence Community—and in particular, the Intelligence Community's current capabilities to combat the terrorist threat—revealed other shortcomings in the way in which information is communicated between and among intelligence agencies.

Our study is hardly the first to identify the need for information sharing, both within the Intelligence Community and in other areas of the government.[3] The Intelligence Community has taken its own steps to address the problem internally, and has launched more than 100 initiatives since September 11 to

improve information sharing.[4] While some of these steps deserve praise, progress has been uneven and sporadic. As demonstrated in our terrorism case study, the Terrorist Threat Integration Center, now absorbed within the National Counterterrorism Center, has succeeded in establishing connections to dozens of networks at its new terrorism warning center—but obstacles remain. Representatives from one agency still face legal and policy barriers that prevent them from gaining access to the databases of another.[5] Collectors of information continue to operate as though they "own" the information, and collectors continue to control access to the information they generate.[6] Decisions to withhold information are typically based on rules that are neither clearly defined nor consistently applied, with no system in place to hold collectors accountable for inappropriately withholding information.[7]

In short, while some progress has been made since September 11, we are still quite far from the goal of enabling personnel from across the Intelligence Community to access information from anywhere in the Community through their own network-based connections. In our terrorism case study, we agreed with the recent assessment of the DCI's Information Sharing Working Group, which found that "[a] great deal of energy…is being expended across the [Intelligence Community] to improve information sharing. However, the majority of these initiatives *will not produce the enduring institutional change required to address our current threat environment.*"[8]

Recognizing the incomplete nature of the Intelligence Community's efforts, the President and Congress have taken their own steps in recent months to address the problem. The new reform legislation built upon Executive Order 13356 by mandating the creation of an "Information Sharing Environment" for all "terrorism information," and created a new office—a "Program Manager" who reports to the President—to administer it.[9] The purpose of the Information Sharing Environment is to ensure "the sharing of terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."[10] The new law also recast the Information Systems Council established by Executive Order 13356 as the "Information Sharing Council" with responsibility to oversee the development of the Information Sharing Environment.[11] Most everyone now "gets it"; when we asked the most distinguished leaders of the Intelligence Community to name their first priority for reform, many responded "information sharing." There is broad consensus on the big picture. But the problem is hard to fix. While some technical barriers exist, policy bar-

riers are the real problem. One must not dismiss concerns about security or the protection of sources and methods as illegitimate; but, at the same time, such concerns must not force a stalemate, which is too often the result when interagency initiatives move from rhetoric to implementation.

The initial implementation plan of the Information Sharing Council exemplifies our concern. The President directed the Council, within 120 days, to produce a "plan, with proposed milestones, timetables for achieving those milestones, and identification of resources" to execute the plan.[12] While the initial plan proposes milestones and timetables, the plan lacks specific quantitative metrics by which to measure success or failure over time.[13] In many cases, the Council seems to have defaulted to consensus,[14] which in most cases means that many hard decisions were not made. A senior member of the Information Sharing Council described the Council's product as a "plan to make a plan,"[15] and we agree.

We recognize that, in addressing the information sharing problem, we do not write on a blank slate. Our recommendations therefore will focus on questions of implementation and enforcement. We offer recommendations on how to smooth out ambiguities in information sharing responsibilities that the intelligence reform legislation created, and more generally on how we believe the new Director of National Intelligence should manage the information sharing effort. Success will require strong, centralized leadership and an enforcement regime that is based on clearly defined milestones, carries substantial penalties for failure to meet them, and has minimal tolerance for excuses. The recommendations below offer our views on how to get there.

IMPLEMENTING THE NEW INTELLIGENCE LEGISLATION: DISENTANGLING OVERLAPPING AUTHORITIES

Recommendation 1

The confused lines of authority over information sharing created by the intelligence reform act should be resolved. In particular:

- The Information Sharing Environment should be expanded to encompass all intelligence information, not just terrorism intelligence;

Recommendation 1 (Continued)

- The Director of the National Counterterrorism Center should report to the DNI on all matters relating to information sharing; and
- The overlapping authorities of the DNI and the Program Manager should be reconciled and coordinated—a result most likely to be achieved by requiring the Program Manager to report to the DNI.

There is no shortage of officials who have been charged in recent years with ensuring information sharing across the federal government. Indeed, the intelligence reform act itself assigns substantial—and often overlapping—responsibilities to three people:

- The *Director of National Intelligence* is given "principal authority to ensure maximum availability of and access to intelligence information within the Intelligence Community consistent with national security requirements."[16] The DNI was also given overall information sharing responsibility to develop an "enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture."[17]

- The *Director of the National Counterterrorism Center* shall "provide strategic operational plans...for the effective integration of counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States."[18] The Director of NCTC also has direct responsibility to "disseminate terrorism information" to all appropriate agencies within the Executive Branch and to the Congress.[19]

- The *Program Manager* is "responsible for information sharing across the Federal Government." [20]

Some of these overlapping authorities can be easily addressed. The Director of the NCTC works for the DNI, and notwithstanding the NCTC Director's theoretical right to report to the President on interagency "strategic operational planning,"[21] split authority for sharing intelligence information is a recipe for stalemate. We recommend that the DNI (and the President, if need be) make clear that the Director of the National Counterterrorism Center exercise

his authority to disseminate terrorism information under the supervision of the DNI.

The harder problem concerns the relationship between the DNI and the information sharing program manager. The legislation directs the President to create an Information Sharing Environment that encompasses all terrorism information from all levels of government within the United States, plus terrorism information from the private sector and from foreign nations.[22] The intelligence reform act gives the program manager "government-wide" jurisdiction but responsibility limited to terrorism information, since the Information Sharing Environment is (at least initially) defined in terms of "terrorism information."[23] The program manager has a two-year term, without explicit provision for re-appointment or succession. For the first year, the primary duty of the program manager is to prepare a plan for submission to the President and to Congress.[24] According to the Conference Report on the legislation, Congress intended to consider extension of the program manager position beyond two years after receiving the program manager's recommendations on "a future management structure for the [Information Sharing Environment]."[25] As noted above, the intelligence reform act stipulates that the Information Sharing Council[26] shall "assist the President and the program manager in their duties" with respect to the Information Sharing Environment.[27]

Although the legislation sets lofty goals for the information sharing program manager, it is not clear that the office has the authority needed to implement even the best of plans for the Information Sharing Environment. The program manager's role is, at bottom, only advisory; the statute confers no budget or executive authority over information sharing programs.[28] In the quite likely event of conflicts that cannot be resolved by the program manager, the job of arbitrating interagency disputes will fall to the Office of Management and Budget.[29]

At the same time, the program manager may have just enough authority to interfere with implementation of information sharing throughout the Intelligence Community. The Community is unlikely to adopt one solution for sharing terrorism intelligence and another for sharing intelligence about chemical, biological, and nuclear weapons. As explained by the interim director of the NCTC, the people working the terrorism problem must be able to search all intelligence information for linkages and insights where the terrorist connec-

tion is not obvious.[30] Thus, the program manager's authority over terrorism information could drive, distort, or delay the Intelligence Community's efforts to share all intelligence more effectively.

To resolve this institutional ambiguity, we believe that the program manager's implementation of a government-wide terrorism information space needs to be coordinated with the DNI's responsibilities to drive information sharing within the Intelligence Community. Our view is that optimal coordination will result if the program manager reports to the Director of National Intelligence. With that said, we recognize that there are competing considerations.

First, the program manager was placed outside the Intelligence Community in order to extend information sharing to elements that normally do not exchange information with the Intelligence Community. These include law enforcement agencies (federal, state, local, tribal, and foreign), federal regulatory agencies (*e.g.*, Federal Aviation Administration, Commerce, and Customs) and the private sector. As our terrorism case study demonstrates, the Intelligence Community has struggled to provide terrorism information to state, local, and tribal authorities.[31] Solutions that work in a classified world cannot be used to share data with this vast new audience. Still, much of the terrorism information shared by and among these agencies will originate with or pass through elements of the Intelligence Community. In our view, the DNI is in the best position to balance the need for sharing terrorism information with the need to protect intelligence sources and methods.

A second objection is that the Intelligence Community includes some of the worst offenders where information sharing is concerned. Unfortunately, we question whether the program manager is likely to force hard decisions on the Intelligence Community if the DNI cannot. Unlike with the temporary program manager, intelligence organizations cannot easily wait out the DNI's tenure, plus the DNI has budget, acquisition, and other authorities over some of the largest agencies affected by the information sharing mandate.

In short, we are far more sure of our diagnosis, that the legislation's allocation of responsibilities is unworkable, than of our prescription—granting the DNI authority over the program manager. In the absence of a better prescription, however, we offer what we believe is the most workable approach to this messy problem.

The intelligence reform act provides that the President shall "designate the organizational and management structures that will be used to operate and manage the Information Sharing Environment."[32] This language, in our view, permits the President to incorporate the role of the program manager into the Office of the DNI in order to ensure the necessary leadership and accountability for the Information Sharing Environment.

MANAGING INFORMATION ACCESS, INFORMATION SECURITY, AND INFORMATION TECHNOLOGY

Of course, if the DNI is to exercise such authority, the DNI must demonstrate a commitment and an ability to achieve information sharing across the government. That will not be easy. So far, information sharing among intelligence agencies, even regarding terrorism, is intense but *ad hoc*. As we described in our terrorism case study, terrorism information sharing depends far too much on agency-specific workarounds. There has not been strong leadership or a centralized approach. Agencies have resisted broader solutions for two plausible reasons: first, because of technological incompatibilities; and second, because of security and privacy restrictions on sharing data. Neither of these objections is trivial, but the Community only makes matters worse by allowing them to fester for lack of decisionmaking authority. For that reason, we recommend that responsibility for security and technology issues in the Intelligence Community be combined into a single office reporting directly to the DNI or his principal deputy. This office would oversee and manage the policy, security, and technical dimensions of all information sharing within the Intelligence Community. To make clear that its responsibilities exceed those of the traditional federal government Chief Information Officer, it could be called the Chief Information Management Officer (CIMO).

Recommendation 2

The DNI should give responsibility for information *sharing,* information *technology,* and information *security* within the Intelligence Community to an office reporting directly to the DNI or to the Principal Deputy DNI.

The job of the chief information management officer is to make the difficult decisions that ensure uniform information sharing and security policies across the Intelligence Community. He or she would be responsible for issuing policies and directives for the Information Sharing Environment, empowered to enforce such policies *within* the Intelligence Community, and held accountable for the overall progress of the Information Sharing Environment both within and beyond the Intelligence Community. We also note that the Mission Managers we propose—who would have unique insight into the information that exists in their respective subject areas—could play a key role as advocates for information sharing and as advisors to the CIMO concerning the content of material in the Information Sharing Environment (and who should have access to it).

No Information Sharing Environment can succeed unless it also acts as an information security environment. The chief information management officer must assure both greater sharing of information and the protection of sources and methods. Protection of sources and methods is not only a solemn duty of the intelligence profession, but it is also a matter of survival and the foundation of the Community's success. Even inadvertent compromises can lead to dead agents or the obsolescence of technical systems that cost billions of dollars and take more than a decade to acquire. The risk is clear: adding scores of professionals to an Information Sharing Environment lacking adequate security and information access controls may compromise the Community's intelligence sources and methods.

The potential conflict between network expansion and network security leads to bureaucratic confrontations between their respective advocates. The two camps normally report through separate chains of command that converge only at high levels of institutional management. Hence conflicts of lesser importance that are not worthy of escalation remain unresolved and result in paralysis. Those of greater importance are elevated to high-level managers who typically have broad responsibilities well beyond adjudication of network or information access issues, and precious little time or attention to work the problems. Until the recent push for information sharing, the security contingent held all the trump cards. No one was held accountable for failure to share information; but the opposite was true for a security failure.

Finding the right compromise between information sharing and information security is a question of risk management. Each of these values should be

accorded its proper weight, with due recognition of the increased importance of information sharing in the current threat environment. Successful execution of this risk management function requires hands-on, continuous planning and leadership—not disjointed and occasional adjudication by committee. Accordingly, we recommend that responsibility within the Intelligence Community for both information *sharing* and information *security* (protection of sources and methods) reside with the DNI, delegable to the chief information management officer. The CIMO would be held accountable for the effective development of the shared information space, using risk management to achieve the right balance between sharing and security. The dual responsibilities of this office would encourage planning and decisions based on overall mission objectives and accountability to the diverse needs of Information Sharing Environment users.

LEARNING FROM PAST INFORMATION SHARING EXPERIENCE

We do not propose to tell the DNI and the chief information management officer how to resolve all of the difficult technical and policy issues associated with creating an Information Sharing Environment that works. Nonetheless, we can offer some insights that may be of use as the DNI sets forth on this difficult endeavor. Many of these insights arise from the Intelligence Community's experience with Intelink, which functions as a kind of Internet for the secure sharing of intelligence in parts of the Intelligence Community.

Recommendation 3

In designing an Information Sharing Environment, the DNI should, to the extent possible, learn from and build on the capabilities of existing Intelligence Community networks. These lessons include:

- The limitations of "need to know" in a networked environment;
- The importance of developing mechanisms that can protect sources and methods in new ways;
- Biometrics and other user authentication (identification) methods, along with user activity auditing tools, can promote accountability and enhance counterintelligence capabilities;

Recommendation 3 (Continued)

- System-wide encryption of data can greatly reduce the risks of network penetration by outsiders; and
- Where sensitive information is restricted to a limited group of users, the Information Sharing Environment should ensure that others searching for such information are aware of its existence and provided with a point of contact who can decide quickly whether to grant access.

First, it is unrealistic to think that we can achieve our information sharing goals without departing from traditional approaches to the "need-to-know" principle. Under the current rules, each government official who holds classified information has a responsibility "to ensure that a need-to-know exists" before giving access to another person, even if that person has all the requisite clearances.[33] In practice, these individual decisions follow agency-specific policies (or unstated habits) that vary widely across the Intelligence Community. If rigidly applied, the "need-to-know" rule is incompatible with a networked environment. In a networked environment, providers of information cannot know for sure when a user "needs" a particular piece of information. Instead, as the Intelink experience demonstrates, users of this service must be given access to all information broadly available on the network within the clearance levels of the individual user, and consistent with applicable privacy and civil liberties guidelines. Intelink provides the Intelligence Community with classified services analogous to those of the World Wide Web on the Internet.[34] It provides easy user access, security and privacy safeguards, information discovery and search, collaboration through e-mail and chat rooms, and automated, personalized information delivery.[35] Other existing information sharing networks include JWICS (up to Top Secret/Sensitive Compartmented Information), SIPRNet (up to Secret/collateral information), and OSIS (Sensitive But Unclassified and For Official Use Only).

At the same time, one must not dismiss the risks of this approach. Moving to an Information Sharing Environment requires additional safeguards. Strong authentication, careful audits of user behavior, including inquiries into the reasons for accessing a particular report, will all help to safeguard the system from compromise. In addition, even in a generally open environment, information of extraordinary sensitivity will have to be restricted to limited groups or to "communities of interest" with proper clearances.[36] For example, infor-

mation access controls could limit viewing privileges for a particular document to a list of named individuals, with enforcement facilitated by requiring biometric identification of each user prior to viewing the document. The CIA has already established a "trusted network" on Intelink that permits the automated distribution of highly sensitive "blue border" reports to pre-approved individuals.[37]

But the proliferation of communities of interest raises another problem. What if an analyst is searching for—and needs to know—information that is hidden in an access-controlled database? How does the analyst even know whom to ask for access? One solution proposed for this problem is to make available a catalog of all the communities of interest in the Information Sharing Environment, functioning much like a library catalog in that it provides an access number and a brief summary of the information contained in these areas (much like controlled or reserved stacks at public libraries). While such an approach may not suit all situations—sometimes even the summary descriptions will be too sensitive to share widely—it could enhance the ability of analysts to access information they need.

Similarly, Intelink has not yet reached its full potential because some agencies still do not make much of their reporting available through the Intelink system. The reluctance of some agencies to connect their information systems and databases with outside systems such as Intelink stems not simply from a lack of interagency trust. Some agencies, notably NSA, provide intelligence officers from trusted partner nations with access to their networks, while agencies such as CIA resist sharing information about human assets with any foreign nationals for fear of compromising sources and methods. The Intelligence Community can resolve this tension by requiring stronger authentication procedures for all users of Intelink and similar systems, and by enabling users to establish communities of interest—essentially, highly secure virtual workspaces—that shield particularly sensitive information from all users except those who have been admitted by name. Authentication methods using biometrics and digital certificates offer excellent protection against unauthorized information access, since they can establish with near certainty the identity of the person attempting to access a given system. Emerging software-based auditing tools that monitor the behavior of users can help security officers spot suspicious activity and further strengthen the integrity of Intelink and related information systems.

As has been recognized by the Markle Foundation in some detail, such automated accountability technologies would greatly strengthen counterintelligence capabilities as well as protecting privacy.[38] Modern encryption can provide additional security by effectively precluding the deciphering of internal communications by persons outside the network. Control checks, such as identity management systems, can check each user's access privileges and either admit them, deny them access, or provide a security point of contact to adjudicate the matter virtually. Additional security might be provided by considering greater use of "thin clients," where all data is stored on servers remote from the user, and user terminals have no interface for removable media (*i.e.*, no ability to write to a CD).

All of these technologies are available off the shelf today. Experience with Intelink suggests that sometimes the best approach is to "just do it." Without having studied the information sharing implementation plans of the agencies concerned, we cannot say that this is the only way forward. But building on the lessons learned through the use of Intelink and current networks with information sharing capabilities offers many advantages.

SETTING UNIFORM INFORMATION SHARING POLICIES

The fundamental barriers to information sharing are not a matter of technology; they arise from the legal, policy, and cultural "rules" that pervade the system. That is why information sharing cannot be a matter of issuing one edict or adopting one technology. It requires a patient sorting out of many complex policy threads and adapting systems and policies to emerging Intelligence Community and government processes. Without pretending that we have identified all of the problems, let alone all of the solutions, we have been able to isolate several of the policies that stand in the way of information sharing. In many cases we suggest solutions to these problems.

Recommendation 4

Primary institutional responsibility within the Intelligence Community for establishing clear and consistent "U.S. persons" rules should be shifted from individual collection agencies to the Director of National Intelligence. These rules would continue to be subject to the Attorney General's review and approval. To the extent possible, the same rules should apply across the Intelligence Community.

The rules governing collection and retention of information on "U.S. persons" are complicated, subject to varying interpretations within each agency, and differ substantially from one agency to the next.[39] These rules, in practice, often pose substantial impediments to analysts accessing "raw data" in the possession of particular collection agencies. We believe that practical responsibility for authoring and periodically reviewing these "U.S. persons" rules should be shifted from individual collection agencies to the DNI, subject to statutory review and approval by the Attorney General.[40] Vested with this responsibility, the DNI would ensure that these rules are consistent across agencies, that they are periodically reviewed and updated to account for new collection technologies and analytic tools, and that they accurately encapsulate statutory and constitutional privacy protections enshrined in law. As we note in Chapter Six (Leadership and Management), we suggest that the DNI vest primary responsibility for harmonizing and reviewing these rules within the Office of the DNI's General Counsel.

Recommendation 5

The DNI should set uniform information management policies, practices, and procedures for all members of the Intelligence Community.

Current agency-specific policies and practices do not suit a modern, networked environment. For example, criteria for certifying networks and software for use on networks differ from one agency to the next. The Intelligence Community lacks common standards for firewalls and network gateways. [41] Uniform standards and procedures should govern submission of documents and information to the Information Sharing Environment; submission of information to the sharing environment should be an obligation, not a choice.

To enable users from across the Intelligence Community to access quickly the information they need, the DNI will need to standardize data and meta-data formats, as well as procedures for adjudicating disputes.

Recommendation 6

All users of the Information Sharing Environment should be registered in a directory that identifies skills, clearances, and assigned responsibilities of each individual (using aliases rather than true names when necessary). The environment should enable users to make a "call for assistance" that assembles a virtual community of specialists to address a particular task, and all data should be catalogued within the Information Sharing Environment in a way that enables the underlying network to compare user privileges with data sensitivity.

At present, the Intelligence Community has no comprehensive online directory of analysts and technical experts. Our case studies—particularly Iraq, Afghanistan, and Terrorism (Chapters 1, 3, 4)—and our discussion of intelligence analysis (Chapter 8), highlight the need for ongoing communication and interaction among analysts, and for "communities of interest" that can form, adapt, and dissolve in response to specific issues or tasks. For example, a Mission Manager examining collection on biological weapons in Asia should be able to find and call on all analysts in other Intelligence Community agencies who have an expertise in biological weapons or an Asian regional specialty. Analysts' biographical profiles, previous analytic reporting output, and contact information should be readily accessible to the Mission Manager through the Information Sharing Environment.

Recommendation 7

The DNI should propose standards to simplify and modernize the information classification system with particular attention to implementation in a network-centric Information Sharing Environment.

Finally, the rules governing classification of national security information are antiquated and overly complex. As we noted in our terrorism case study, caveats such as ORCON ("originator controlled") wrongly imply that collectors of

intelligence "own" the information and should control access to it.[42] The compartmentation of highly sensitive activities creates unknown islands of information under the "personalized"[43] security governance of each program manager. For understandable reasons, collectors have historically accorded paramount importance to protection of sources and methods and have given insufficient weight to information dissemination and "sharing." This culture of diffused information ownership has resulted in inconsistent information access standards and arbitrary enforcement of those standards.

The DNI should move toward a culture of "stewardship" of intelligence information instead of ownership. Federal government information belongs to the nation and is entrusted to the Intelligence Community in order to pursue the nation's best interest. Collectors of intelligence information should not control access to such information; the DNI or the DNI's designee should exercise that authority. As a baseline standard or norm, the DNI should require the submission of all intelligence information, with proper classification controls, to the Information Sharing Environment. Those who seek to exclude particular information from the environment must carry the burden of proving that such exclusion is clearly in the nation's interest.

EMPLOYING STRONG ENFORCEMENT MECHANISMS AND INCENTIVES TO DRIVE CHANGE

The Information Sharing Environment envisioned by the President and Congress faces innumerable pragmatic obstacles to speedy implementation. Transition to new technology, new data standards, and new procedures will disrupt existing agency functions, some of which may serve a vital national security role. For critical systems, it may be necessary to create a parallel infrastructure for the Information Sharing Environment, keeping legacy systems fully operational until the new one is built, tested, and ready for switch-over. Agencies will procrastinate for fear of degrading mission performance. Security apprehensions will sprout. The DNI will need to drive change relentlessly or the sharing environment will founder.

Recommendation 8

We recommend several parallel efforts to keep the Information Sharing Environment on track:

- ***Collection of metrics.*** The chief information management officer should introduce performance metrics for the Information Sharing Environment and automate their collection. These metrics should include the number and origination of postings to the shared environment, data on how often and by whom each item was accessed, and statistics on the use of collaborative tools and communications channels, among others. Such performance data can help to define milestones and to determine rewards and penalties.
- ***Self-enforcing milestones.*** Milestones should include specific and quantifiable performance criteria for the sharing environment, as well as rewards and penalties for succeeding or failing to meet them. The DNI should empower the chief information management officer to use the DNI's budget, mission-assignment, and personnel authorities to penalize poor agency performance.
- ***Incentives.*** The DNI should ensure that collectors and analysts receive honors or monetary prizes for intelligence products that receive widespread use or acclaim. Users should post comments or rate the value of individual reports or analytic products, and periodic user surveys can serve as peer review mechanisms.
- ***Training.*** The DNI should promote the training of all users in the Information Sharing Environment, with extended training for analysts, managers, and other users of the environment.

PROTECTING PRIVACY AND CIVIL LIBERTIES

No discussion of information sharing initiatives would be complete without noting that the sharing of information has raised privacy and civil liberties concerns in the wake of September 11.

Our recommendations in this chapter rest securely in the belief that all concerned will follow provisions in the new legislation and executive orders that are designed to make the protection of civil liberties an ongoing priority

for the intelligence and law enforcement communities. The recent executive orders establishing the NCTC and mandating greater sharing of counterterrorism information each included the protection of "the freedom, information privacy, and other legal rights of Americans" as part of the underlying policy.[44] And on the same day the President issued these orders, he established the President's Board on Safeguarding Americans' Civil Liberties.[45]

Building on these executive orders, the legislation establishes a Privacy and Civil Liberties Oversight Board within the Executive Office of the President.[46] The Board is tasked with reviewing regulations, policies, and laws relating to counterterrorism, including those that address information sharing, to ensure that each of these takes account of privacy and civil liberties concerns.[47] The Board is also charged with regular reviews of the information sharing practices of the executive branch to address the same concerns.[48]

Further, the new law places a Civil Liberties Protection Officer in the office of the DNI,[49] who, alone among the legislatively-mandated staff, must *directly* report to the DNI.[50] The statute also recommends, although it does not require, that other entities establish similar positions.[51] The officer is specifically charged with ensuring that policies and procedures protect civil liberties, that the use of technology does not erode privacy protections, and that U.S. persons information is handled in compliance with existing legislation.[52]

Provisions of the legislation specifically calling for more information sharing also take care to address privacy concerns. Indeed, the new system must "incorporate[] protections for individuals' privacy and civil liberties."[53] Even before implementation of the new Information Sharing Environment, the President, in consultation with the Privacy and Civil Liberties Oversight Board, must issue guidelines to "protect privacy and civil liberties in the development and use" of the Information Sharing Environment.[54] And the separate implementation plan must include a "description of the means by which privacy and civil liberties will be protected in the design and operation" of the Information Sharing Environment.[55] Further underscoring the centrality of this issue, the Program Manager for this effort must "ensure the protection of privacy and civil liberties" when he sets policies and procedures for information sharing.[56] And oversight of this issue will be ongoing. The President's annual report to Congress on the status of information sharing must address, among other things, "actions taken in the preceding year to implement or enforce privacy and civil liberties protections."[57]

Thus, the law already provides the framework for appropriate protection of civil liberties in the context of information sharing. Adequate protection will, however, require detailed implementation in the development of the system itself, perhaps assisted by the oversight board and privacy experts and groups outside the Intelligence Community. In our view, an equally important protection is in the technology and the culture of the agencies that do the sharing. Much new technology can be used effectively to protect information from misuse. The intelligence reform act recognizes this possibility by calling for the use of audit, authentication, and access controls in the Information Sharing Environment.[58] These technologies impose accountability on every user of the Information Sharing Environment. They also allow agencies to know who is accessing particular files and to determine, in advance or after the fact, whether access is proper. Data can be tagged to identify which people or organizations are entitled to access it, and strong authentication can dramatically reduce the risk that an unauthorized user will gain access. Auditing techniques allow the system to find users whose access is unusual or not clearly justified and to alert supervisors or security personnel to the need for further investigation—a technique that is unavailable when information is shared by paper. All of these techniques can provide added privacy protection for Americans.

The pursuit of privacy and national security is not a zero-sum game. The same technologies that protect against violations of privacy can also provide strong counterintelligence capabilities—something that will be essential if the Information Sharing Environment is to work over the long run. As the Markle Foundation plainly put it, any information sharing system must come with mechanisms designed to foster trust, "[f]or without trust, no one will share."[59]

ENDNOTES

[1]For example, CIA failed to pass names of suspected terrorists to the Federal Aviation Administration and Customs, and the FBI failed to disseminate a warning from its St. Louis Field Office to any other agency. *Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004) (hereinafter "9/11 Commission Report") at p. 258.

[2] Chapter One (Iraq).

[3] *See generally* 9/11 Commission Report; Markle Foundation Task Force, *Creating a Trusted Information Sharing Network* (Dec. 2003).

[4] DCI Community Management Staff, *Calibration Report: Community Intelligence Community Collaboration and Information Sharing to Win the War on Terrorism: Phase 1* (May 2004) (unclassified excerpt) (hereinafter "IC May 2004 Calibration Report").

[5] Chapter Four (Terrorism).

[6] *Id*.

[7] *Id.*

[8] IC May 2004 Calibration Report at p. ES-1 (emphasis in original).

[9] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1016, Pub. L. No. 108-458 (hereinafter "IRTPA").

[10] *Id.* at § 1016(b)(2).

[11] *Id.* at § 1016(a)(1).

[12] Executive Order 13356 (Aug. 27, 2004) at § 5(c).

[13] The failure of the Information Sharing Council to specify quantitative metrics for accountability may have resulted from the overlap in responsibilities between the Council as provided by Executive Order 13356, and those of the Program Manager as provided by the Intelligence Reform Act of 2004.

[14] The Information Sharing Council report is replete with phrases like "mutually satisfactory approach." See generally Information Systems Council, *Initial Plan for the Interoperable Terrorism Information Sharing Environment* (Dec. 20, 2004) (hereinafter "ISC Report").

[15] Interview with Department of Defense counterintelligence and security official (Feb. 8, 2005).

[16] IRTPA at § 1011 (amending § 102A of the National Security Act).

[17] *Id.*

[18] *Id.* at § 1021.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.* at § 1016(b).

[23] While the act gives the information program manager responsibility (without limitation) for "information sharing across the Federal Government," the provisions creating this office are in the context of legislation that deals only with "terrorism information" as expressly defined. IRTPA at § 1016(a)(4).

[24] *Id.* at § 1016(f)(1).

[25] In discussion of the Conference Report, Senator Collins stated: "The legislation provides that the program manager is to serve for two years, during the initial development of the ISE, to ensure that the project gets off to a sound start. As part of the implementation plan to be submitted to Congress after one year, the program manager is to recommend a future management structure for the ISE, including a recommendation as to whether the position of program manager should continue." *Congressional Record—Senate* (Dec. 8, 2004) at p. S11973.

[26] This and future references in the text to the Information Sharing Council refer to the legislatively created body; previously the term referred to the one created by Executive Order.

[27] IRTPA at § 1016(g)(1).

[28] The legislation provides that the Program Manager will "assist in the development of policies, procedures, guidelines, rules and standards" for the ISE. *Id.* at § 1016(f)(2)(A).

[29] Executive Order 13356 established the Information Systems Council, chaired by the Office of Management and Budget, and directed it to "report to the President through the Assistants to the President for National Security Affairs and Homeland Security." Executive Order 13356 (Aug. 27, 2004) at § 5(c). IRTPA renamed the "Information Systems Council" to be the "Information Sharing Council" and gave it responsibility to "assist the President and the program manager in their duties" with respect to information sharing. IRTPA at § 1016(g)(1).

[30] Interview with senior National Counterterrorism Center official (Feb. 8, 2005).

[31] Chapter Four (Terrorism).

[32] IRTPA at § 1016(b)(1)(B). We do note, however, that in the discussion of information sharing in connection with the Conference Report on the intelligence reform act, Senator Collins stated, "It is not our intent that the DNI also assume further responsibilities of program manager." *Conference Report—Senate* (Dec. 8, 2004) at p. S11973.

[33] Executive Order 12968 (Aug. 4, 1995) at § 2.5(b).

[34] Many of the future "milestones" described in the Information Sharing Council's report have already been achieved by Intelink: "At the core of this interoperable terrorism sharing environment, is an environment resembling the Internet. The environment would have a variety of sites managed by participating organizations with tools to help link users (*i.e.*, information producers and consumers) with the information they need. Unlike the Internet, however, this is not a loose, voluntary association of parties, but rather a disciplined structure for the creation, protection, dissemination, retention, and use of actionable information across seven related communities." ISC Report at p. 24.

[35] The Information Sharing Council's report describes Intelink services on JWICS and SIPRNET as follows: "The networks provide sophisticated search and discovery capabilities, support email and collaboration, and maintain directories and other services making it easy for users to find and use information." *Id.* at p. 35.

[36] This is done by metadata tags specifically referencing the identity of individuals authorized to have access to a particular document.

[37] Interview with CIA counterintelligence officials (Jan. 27, 2005).

[38] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Information Sharing Network* (Dec. 2003) at p. 140.

[39] "Agencies within the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures estab-

lished by the head of the agency concerned and approved by the Attorney General." Executive Order 12333 (Dec. 4, 1981) at § 2.3.

[40] This might require a change to Executive Order 12333, which directs individual agencies to establish their own U.S. persons rules (subject to Attorney General approval) and does not expressly interpose the DNI in that process. As we note in Chapter Ten (Intelligence at Home), our envisioned Assistant Attorney General for National Security would be the natural office to take the lead in securing Justice Department approval of such guidelines.

[41] Interview with Department of Defense counterintelligence and security official (Feb. 8, 2005).

[42] Chapter Four (Terrorism).

[43] The program managers of Special Access Programs have wide discretion to set security rules applicable only to their program.

[44] Executive Order 13354 (Aug. 27, 2004) at § 1(b); Executive Order 13356 (Aug. 27, 2004) at § 1(b).

[45] Executive Order 13353 (Aug. 27, 2004).

[46] IRTPA at §1061.

[47] *Id.* at § 1061(c)(1).

[48] *Id.* at § 1061(c)(2).

[49] *Id.* at § 1011.

[50] *Id.*

[51] *Id.* at § 1062.

[52] *Id.* at § 1011.

[53] *Id.* at § 1016(b)(2)(H).

[54] *Id.* at § 1016(d)(2)(A).

[55] *Id.* at § 1016(e)(8).

[56] *Id.* at § 1016(f)(2)(B)(viii).

[57] *Id.* at § 1016(h)(2)(H), (I).

[58] *Id.* at § 1016(b)(2)(I).

[59] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security* (Dec. 2, 2003) at p. 18.

CHAPTER TEN
INTELLIGENCE AT HOME: THE FBI, JUSTICE, AND HOMELAND SECURITY

Summary & Recommendations

Combating chemical, biological, and nuclear terrorism, as well as other foreign intelligence challenges, will require intelligence assets both inside and outside the United States. As the events of September 11 demonstrated, we cannot afford a wall that divides U.S. intelligence efforts at the border. Although the FBI is making progress toward becoming a full member of the Intelligence Community, it has a long way to go, and significant hurdles still remain. In our view, the FBI has not constructed its intelligence program in a way that will promote integrated intelligence efforts, and its ambitions have led it into unnecessary new turf battles with the CIA.

Meanwhile, the Department of Justice has not yet put its national security components in one office; its anti-terrorism and intelligence support offices are as scattered as they were on September 10, 2001. And the Department of Homeland Security is still following a Treasury Department order from the 1980s that requires high-level approval for virtually all information sharing and assistance to the Intelligence Community.

In light of these problems we recommend that:

- The FBI create a new National Security Service within the Bureau and under a single Executive Assistant Director. This service would include the FBI's Counterterrorism and Counterintelligence Divisions and its Directorate of Intelligence, and would be subject to the coordination and budget authorities of the DNI;
- The DNI ensure that there are effective mechanisms for preventing conflicts and encouraging coordination among intelligence agencies in the United States;
- All intelligence activity within the United States—whether conducted by the CIA, FBI, or Department of Defense—remain subject to Attorney General guidelines designed to protect civil liberties;

Summary & Recommendations (Continued)

- The Department of Justice consolidate its national security elements—the Office of Intelligence Policy Review, and the Counterterrorism and Counterespionage sections—under a new Assistant Attorney General for National Security; and
- The Department of Homeland Security rescind Treasury Order 113-01.

INTRODUCTION

The events of September 11 made clear that terrorists can operate on both sides of the U.S. border. Terrorists are seeking nuclear and biological weapons outside the United States, but they long to use them here.

This new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had on September 10, 2001. It is these two tasks to which we now turn.

CHANGE AND RESISTANCE TO CHANGE AT THE FBI

It has now been three and a half years since the September 11 attacks. A lot can be accomplished in that time. Three and a half years after December 7, 1941, the United States had built and equipped an army and a navy that had crossed two oceans, the English Channel, and the Rhine; it had already won Germany's surrender and was two months from vanquishing Japan.

Change

The FBI has spent the past three and a half years building the beginnings of an intelligence service and striving to transform itself into a hybrid law enforcement and intelligence agency.[1] Field offices now routinely cull intelligence information from operations and investigations, and disseminate Intelligence

Information Reports. An intelligence official from another law enforcement agency praised the FBI's ability to extract pertinent information from cases, pointing out that "[t]hey are doing a better job than anybody could have expected."[2] The Bureau has developed new intelligence training courses, Field Intelligence Groups to supervise intelligence production, and an expanded analytic cadre. FBI headquarters has hired hundreds of analysts and agents from outside its traditional core competencies (law enforcement, accounting, and the military).[3] In 2003 Director Mueller appointed an Executive Assistant Director for Intelligence to preside over these efforts and lead the newly created Office (now Directorate) of Intelligence. These are no small accomplishments.

At the same time, determination at the top of the organization does not always translate into change in the field. FBI Directors, no less than outsiders, must contend with a bureaucratic culture that naturally resists change. We are not the first to see the problem. The 9/11 Commission noted with some concern that it had "found gaps between some of the announced reforms and the reality in the field."[4]

Past efforts to build a strong intelligence capability within the FBI have foundered on this resistance. In 1998 and 1999, similar reforms[5] failed in quick succession as a result of strong resistance from the FBI's operational divisions and an intelligence architecture that could not defend itself inside the bureaucracy.[6] Several of the obstacles FBI has faced in reforming itself stem from the Bureau's long and proud law enforcement culture. While the Bureau is making progress toward changing its culture, it remains a difficult task and one that we believe will require more structural change than the Bureau has instituted thus far.

As America's premier federal law enforcement agency, the FBI's law enforcement legacy is strong. Law enforcement work has long been the surest route to professional advancement within the Bureau. Even now, only nine of the heads of the FBI's 56 field offices come from divisions other than the Criminal Division.[7] And many field offices are still tempted to put law enforcement ahead of intelligence-gathering, betting that "Bin Laden is never going to Des Moines."[8] This is understandable—local political and other external forces often press the Bureau to focus on its criminal law enforcement responsibilities. As one Special Agent in Charge explained, when a local law enforcement agency calls for help, "you never want to say no."[9]

Resistance to Change

So, the question remains: can the FBI's latest effort to build an intelligence capability overcome the resistance that has scuppered past reforms? In our view, the effort this time is more determined, but the outcome is still in doubt.

Here we highlight three areas critical to intelligence work—analytic capability, validation of human sources of intelligence (*i.e.*, asset validation), and information technology—in which the FBI has made significant but, in our view, insufficient progress.

First, the FBI is still far from having the strong analytic capability that is required to drive and focus the Bureau's national security work. Although the FBI's tactical analysis has made significant progress, its strategic capabilities—those that are central to guiding a long-term, systematic approach to national security issues—have lagged.[10] And while the FBI maintains the ambitious goal of improving its strategic analysis—creating a Strategic Analysis Unit in the Directorate of Intelligence and a strategic analysis function in each Field Intelligence Group by 2005[11]—every indication is that the Bureau will have difficulty meeting this worthy objective, particularly at the field level. This is because the Bureau has largely been unable to carve out time for its analysts in the field to do long-term, strategic analysis. According to a 2004 evaluation of one Field Intelligence Group, "because of the current structure and manpower constraints, nearly all analysis is limited to the tactical level supporting individual cases."[12] A 2005 National Academy of Public Administration study on the FBI forecasts that "even after a larger analytical staff is built, the tendency will be for immediate operational demands to push out strategic analyses."[13] To place the Bureau's current production in context, consider that the FBI currently publishes approximately a quarter as many long-term (non-current) analytic pieces as CIA does in a given year.[14]

This is not to suggest that the Bureau should replicate CIA's model. The Bureau's field office structure makes the FBI unique. One senior official emphasized that FBI has an operational emphasis that disproportionately requires actionable intelligence.[15] But although we are sympathetic to the FBI's particular analytic needs, we remain concerned that the current structure of the FBI's intelligence program, and the relationship between analysts and field operations, will not encourage analysts to rise above individual investigations, develop subject matter expertise, or *drive*—and not merely

inform—counterintelligence, counterterrorism, and foreign intelligence collections, investigations, and operations.

The Bureau must also overcome a long history of treating analysts as "support staff." In the field offices there have always been two main categories of personnel: agent and non-agent (or "support"), and there is little doubt that agents enjoy preeminent status. As a 9/11 Commission staff statement noted, several field analysts complained that they "were viewed as 'uber-secretaries,' expected to perform any duty that was deemed non-investigative, including data entry and answering phones."[16] Even today, there is still evidence of analysts' subordinate role. As just one example, according to a 2004 report on one field office, "due to a backlog of telephone numbers to be loaded into telephone applications, the FIG [Field Intelligence Group] has requested overtime and pulled analysts from squads to load and analyze data…[T]he use of [Intelligence Analysts] for clerical duties diminishes the analytical function of an [Intelligence Analyst]."[17] We expect the FBI will struggle to get its analytic cadre where it needs to be, in part because the Bureau must compete with other, better-established analytical entities within the Intelligence Community for analytic resources.[18]

A second area that requires further reform is the system by which the FBI attempts to validate human sources of information, commonly referred to as "asset validation." For any organization that collects human intelligence, having an independent system for asset validation is critical to producing reliable, well-vetted intelligence. Indeed, the Intelligence Community's failure to validate assets adequately and communicate fabrication notices properly proved especially costly in the Iraq WMD debacle.[19]

Over the past several years the FBI's Counterintelligence Division has instituted a sophisticated and intensive system for asset validation. This initiative deserves praise, but the FBI has not yet instituted this system in its other operational divisions.[20] Director Mueller and the head of FBI's Counterterrorism and Counterintelligence Divisions have both stated their intentions to establish comparable systems in the Counterterrorism and Criminal Divisions, but these plans have yet to be implemented.[21] When we asked agents in the field about the FBI's asset validation, we received answers indicating that asset validation remains largely controlled by the field offices.[22] Indeed, when we asked the FBI for a summary of how many assets had been terminated in the last year because they had been judged to be fabricators, we were told that an

answer would take time since a request first had to go out to each of the field offices and then analyzed back at headquarters.[23] This response strongly suggests that the FBI still lacks a centrally-managed database of its human assets—an essential element of any objective and systematic approach to asset validation.

Finally, further reforms are also necessary in the FBI's information technology infrastructure, which remains a persistent obstacle to successful execution of the FBI's national security mission. We believe that the Bureau's failure to develop efficient mechanisms for information sharing both inside and outside the FBI seriously undermines the Bureau's ability to perform its intelligence work. As early as 2002, Senator Richard Shelby highlighted the FBI's failure to develop information technology tools adequate to support its national security mission as a serious shortcoming.[24] Recently the FBI declared that it will largely abandon the Virtual Case File system it had been developing for the past four years at a cost of $170 million. Although Director Mueller claimed in May 2004 that the system was expected to be completed by the end of the year,[25] at about the same time the National Research Council concluded that the FBI's information technology modernization was "*not* currently on a path to success" and that the Virtual Case File System should not be the foundation for the FBI's "analytical and data management capabilities for the intelligence process"—in part because the system was designed to serve the criminal investigative mission rather than the intelligence mission.[26]

Beyond the shortcomings of these individual intelligence capabilities, some of the FBI's achievements in gathering intelligence within the United States raise questions about its ability to focus its intelligence efforts effectively. The Bureau has a remarkable ability to amass resources for a particular task, but its efforts may be poorly tuned. For example, in 2002 the FBI undertook a large-scale effort to interview all recent Iraqi immigrants to the United States in hopes of uncovering foreign intelligence and counterterrorism information that might contribute to the war effort.[27] This huge effort did produce some useful intelligence, but it required countless FBI investigators and many months. Although the project was coordinated with other intelligence agencies in FBI's Joint Terrorism Task Forces, it is less clear to us whether the effort made effective use of strategic analysis or targeting—and the scale of the interview program produced considerable civil liberties controversy.

INTEGRATING THE FBI INTO THE INTELLIGENCE COMMUNITY

The FBI's intelligence capabilities plainly require continued attention. But strengthening the FBI's national security capabilities is not the only task at hand. The FBI must also interact effectively with the rest of the Intelligence Community. The FBI has 1,720 professional intelligence analysts,[28] more than 12,000 agents capable of collecting valuable information in the field,[29] and the primary responsibility for counterintelligence and counterterrorism in the United States.[30] As such, it is a large and critical contributor to U.S. intelligence efforts.

The need for better intelligence coordination across the foreign-domestic divide was identified by the 9/11 Commission and was a moving force behind the *Intelligence Reform and Terrorism Prevention Act*. Creating a DNI with explicit responsibility for coordinating and managing domestic and foreign intelligence agencies serves as an important step in the right direction. But the legislation cannot create a community by itself. In fact, if nothing is done, a determinedly independent FBI could largely elude the DNI's intended authorities. To understand the risk, it is necessary to understand the mechanisms by which the DNI is expected to lead the Intelligence Community.

In writing the intelligence reform legislation, Congress did not create a Secretary of Intelligence or move all of the intelligence agencies under the direct command of the DNI. Congress left the intelligence agencies where they were—the Defense Department in most cases—but it also granted the DNI substantial authority over those agencies. NSA is typical. Though it is a Defense Department agency, NSA is part of the Intelligence Community. To ensure that NSA is responsive to the DNI, Congress gave the DNI significant authority over both NSA's budget[31] and a say in the appointment of its director.[32] The intelligence reform law applies the same basic authorities to the FBI but, in the case of the FBI, the DNI's principal tools for ensuring influence remain troublingly vague.

The DNI's Budget Authority Over the FBI

As a general matter, the DNI's budget authority over parts of the Intelligence Community is significant. The DNI prepares and has reprogramming authority over the National Intelligence Program (NIP, formerly the National Foreign

Intelligence Program, or NFIP). The DNI also ensures that the NIP budget is effectively executed, and monitors its implementation.[33] This picture is, however, far less clear vis-à-vis the FBI. We fear that the DNI may find it difficult—if not impossible—to impose the level of accountability envisioned by the legislation because the FBI's budget is not configured to allow effective Intelligence Community oversight.[34] And in our view, nothing in the Bureau's internal reforms since September 11 has altered this fact.

Approximately a third of the Bureau's total budget is funded through the National Intelligence Program.[35] The vast majority of this money is allocated to the FBI's Counterterrorism and Counterintelligence Divisions.[36] In stark contrast, none of the NIP budget goes to the Bureau's Directorate of Intelligence.[37] Thus, if the current arrangement stands, the DNI will have no budget authority over the office that the Bureau has put at the center of its efforts to develop an intelligence capability.

And this curious arrangement appears even odder when one considers where NIP money goes in light of the DNI's personnel authority over the FBI. In those cases in which an FBI component *does* receive NIP money (*e.g.*, for the Counterterrorism or Counterintelligence Division budgets), the DNI has *no* say in selecting the individual who runs that component. On the other hand, in the one case in which the DNI *does* have a say over an FBI official's appointment (*i.e.*, the Executive Assistant Director of Intelligence),[38] that official's office (*i.e.*, the Directorate of Intelligence) *doesn't* get NIP money. This strikes us as a peculiar arrangement, and one that diminishes the DNI's ability to ensure that the FBI is fully integrated into the Intelligence Community.

This rather confused budgetary situation is further complicated by FBI's internal budget categories. As required by the intelligence reform act, the FBI parses its budget into four parts: intelligence, counterterrorism/counterintelligence, criminal justice services, and criminal enterprises/federal crimes.[39] There is, however, only a small overlap between the National Intelligence Program budget and the Bureau's internal intelligence budget component—what it calls its "Intelligence Decision Unit."

Thus, when the FBI says that the Executive Assistant Director of Intelligence—again, the person over whom the DNI has some personnel authority—has "full control" over the "resources" of the Intelligence Decision Unit,[40] this says very little about the Executive Assistant Director's authority

over National Intelligence Program funds. This is aptly illustrated by the fact that the Intelligence Decision Unit contains less than a third of the Bureau's NIP funds, and that a significant portion of Intelligence Decision Unit dollars go to parts of the FBI that are wholly unrelated to national intelligence programs.[41] In short, simply because something is in the FBI's "intelligence" budget gives little indication of whether the money is relevant to the Intelligence Community or, more importantly, to the DNI.

Not only is the Bureau's internal "intelligence" budget unit not aligned with the Bureau's NIP appropriations, we also doubt that the head of the Directorate of Intelligence actually has even the limited budget authority claimed by the FBI over what it internally describes as the "intelligence" budget. While the FBI states that the Executive Assistant Director for Intelligence "oversees" the Intelligence Decision Unit,[42] it remains unclear whether the Executive Assistant Director will actually have direct authority to formulate, direct, or reprogram the Intelligence Decision Unit budget. This is because, according to an official at the Office of Management and Budget, the Directorate of Intelligence only has unilateral authority over that percentage of the Intelligence Decision Unit that goes directly to the Directorate of Intelligence itself.[43] This means the Directorate has direct authority over only about *four percent* of the Bureau's own "intelligence" budget.[44] Fully 96 percent of the Intelligence Decision Unit falls outside the Directorate of Intelligence, in divisions like Counterintelligence and Counterterrorism.[45]

Hence, although the FBI's Executive Assistant Director for Intelligence may provide input into policy-related decisions regarding the Intelligence Decision Unit, the Executive Assistant Director will not, for instance, control the salaries of those included in the unit, or have budget execution authority over the unit as a whole.[46] So, while the Bureau states that "[a]ll of [its] efforts to create and manage the FBI intelligence budget are directed at ensuring that the DNI is able to exercise oversight of all intelligence spending,"[47] it is rather doubtful that creating the Intelligence Decision Unit—or providing the Executive Assistant Director for Intelligence general oversight over it—accomplishes this goal.

In our view, the FBI's budget process should be organized in a way that unambiguously ensures the responsiveness of the FBI's national security elements to the DNI. This means two things. First, the National Intelligence Program budget should include the budgets of the Directorate of Intelligence—as well

as the Counterintelligence and Counterterrorism Divisions (perhaps excluding purely domestic terrorism work). Second, the DNI should have personnel authority over the FBI official who is responsible for all National Intelligence Program budget matters within the FBI. The current arrangement is far from this ideal.

Instead, the confused allocation of resources, combined with the questionable budgetary authority of the one FBI official over whom the DNI exercises some personnel authority, threatens to undermine one of the DNI's critical "levers of power." If the DNI does not know how NIP funds are allocated and spent by the FBI, and if the DNI does not have some personnel authority over the FBI official responsible for managing NIP funds, then he runs the risk of losing the very authority that the legislation was intended to confer. In such a case, the DNI will have to revert to other authorities, and it is to these we now turn.

Appointment Authority and the Weakness of the Intelligence Directorate

Another important tool at the DNI's disposal is appointment authority of Intelligence Community officials. Congress grants the DNI concurrent authority over the appointment of the heads of intelligence agencies such as NSA, NGA, and CIA.[48] In the case of the FBI, however, this authority is diluted. The DNI has no say in the appointment of the Director of the FBI, presumably because the FBI is the "primary criminal investigative agency in the federal government"[49] and the FBI Director spends considerable time overseeing a large law enforcement staff involved in criminal justice matters. Rather than conferring a role in the appointment of the Director of the FBI, the statute gives the DNI a say in the appointment of the Executive Assistant Director for Intelligence.[50]

This is a workable approach if the Executive Assistant Director for Intelligence can direct the resources necessary to accomplish the Bureau's national security mission. Indeed, that seems to have been Congress's plain intent. The intelligence reform law states that the Executive Assistant Director's office (the Directorate of Intelligence) will be responsible for supervising "all national intelligence programs, projects, and activities of the Bureau" and overseeing all "field intelligence operations."[51] Additionally, the legislation states that the Directorate of Intelligence is responsible for strategic analysis,

the intelligence workforce, and coordinating collection against nationally determined requirements.[52] On the other hand, if the Executive Assistant Director does *not* have authority over the FBI's intelligence-gathering activities, then the DNI's ability to influence appointments to that position becomes of minimal import.

Unfortunately, that is the case today. The Directorate of Intelligence itself has no authority to direct any of the Bureau's intelligence investigations, operations, or collections. It currently performs no analysis, commands no operational resources, and has little control over the 56 Field Intelligence Groups, which, according to the FBI, "manage and direct all field intelligence operations."[53]

Instead, the FBI's national security resources, analysts, and collection capabilities are concentrated in the FBI's Counterintelligence and Counterterrorism Divisions and in the field offices. In fact, the FBI is currently configured so that no single individual other than the Director of the FBI (and perhaps his Deputy) has the authority to direct all of the Bureau's national security missions.

Because the DNI's ability to influence the FBI's conduct depends so heavily on the DNI's ability to oversee the Directorate of Intelligence, we looked closely at what authority the directorate has. We conclude that the directorate's *lack* of authority is pervasive. We asked whether the Directorate of Intelligence can ensure that intelligence collection priorities are met. It cannot. We asked whether the directorate directly supervises most of the Bureau's analysts. It does not. We asked whether the head of the directorate has authority to promote—or even provide personnel evaluations for—the heads of the Bureau's main intelligence-collecting arms. Again, the answer was no. Does it control the budgets or resources of units that do the Bureau's collection? No. The DNI's appointment influence over the head of the directorate therefore does little to bring the FBI's national security activities into a fully functioning Intelligence Community.

Setting and enforcing intelligence priorities. The Directorate of Intelligence is responsible for assigning national intelligence priorities to the FBI's field offices. The FBI has officially stated that it both "recognizes and supports the DCI's authority to formulate intelligence collection requirements for the United States Intelligence Community and has issued FBI collection tasking

directives that translate those requirements into actual tasking by the FBI."[54] Yet at the working level, we found that national intelligence requirements were not uniformly understood. As one FBI official in the Directorate of Intelligence put it, the FBI sees these requirements "more as an invitation" to fill collection gaps than as directives.[55] We spoke with agents at the field level who also expressed some confusion about whether these requirements are directive or advisory.[56] The directorate has recognized this problem in internal reports, noting that interviews with personnel in one field office "demonstrated that individuals were still generally not familiar with the published requirement sets."[57] Although a significant part of the problem is that the national requirements system itself does not demand adequate accountability, our concern is that the DNI's attenuated line of authority vis-à-vis the FBI will make this problem particularly acute.

We do not believe this state of affairs is what the 9/11 Commission envisioned when it stressed the need for the FBI "to be able to direct its thousands of agents and other employees to collect intelligence in America's cities and towns."[58] Without control of collection resources, the Directorate of Intelligence lacks the requisite authorities to direct intelligence gathering. Unlike the Counterterrorism, Counterintelligence, Cyber, and Criminal Divisions, the Directorate of Intelligence currently commands no operational resources and has no authority with respect to field operations; it cannot initiate, terminate, or re-direct any collection or investigative operation in any FBI field office or in any of the four operational divisions at FBI headquarters.[59] Additionally, the directorate has no direct authority over the heads of the field offices unless it can somehow prompt the intervention of the FBI Director or his deputy.

Although the FBI has established Field Intelligence Groups in all of its field offices to "manage and direct all field intelligence operations,"[60] the Directorate of Intelligence has little direct control over the field groups either. Nor is it clear that the Field Intelligence Groups will have a real impact on how field offices actually conduct counterintelligence or counterterrorism investigations and activities—the core of FBI's intelligence collection capabilities.[61]

Controlling analysis and related resources. The Directorate of Intelligence also lacks direct supervisory authority over the vast majority of the FBI's analysts. While there are 1,720 intelligence analysts at the Bureau,[62] the Directorate of Intelligence contains just 38 of them.[63] Although the intelligence reform act designates the Directorate of Intelligence as responsible for strate-

gic analysis,[64] the directorate currently does no analysis itself;[65] the 38 analysts in the directorate perform a policy role.[66] (The directorate does, however, coordinate the Director's Daily Brief to the President—a compilation of analytic products that are produced by the operational divisions and packaged by the intelligence directorate for dissemination.)[67]

Furthermore, related resources that do fall under the control of the intelligence directorate may continue to fluctuate. In at least one case, resources that were initially given to the Directorate of Intelligence were later taken away. In early 2004 the Directorate of Intelligence hired a contractor to design and execute a comprehensive intelligence training program. The directorate's ownership of this intelligence training component ended, however, when the FBI's training headquarters at Quantico, Virginia asserted primacy in training matters and directed that it be given ownership of the program.[68] Quantico won the battle, and the Directorate of Intelligence, rather than being able to tailor its own program, was forced into the position of customer. Once again, this illustrates why a line of authority that only connects the DNI to the Bureau through the Directorate of Intelligence may result in the DNI having only tenuous authority with respect to the FBI's national security-related resources.

Exercising promotion and evaluation authority. Lacking significant operational and resource authority, the Executive Assistant Director for Intelligence might turn to personnel authority to manage the Bureau's national security effort. Yet the intelligence directorate has little personnel authority with respect to the Bureau's national security elements. The intelligence directorate's primary leverage comes from its semi-annual review of how headquarters and field offices have utilized intelligence resources—a so-called "program" review.[69] These evaluations do not, however, impose individual accountability for failing to fulfill headquarters-issued requirements, much less control how assets are directed. These after-the-fact reviews therefore have no direct effect on those who lead the execution of the Bureau's national security missions.

With respect to promotions and personnel evaluations, the head of the intelligence directorate is not the performance "rating official" (nor does the head of the directorate share that responsibility) for the component head in any FBI field office or headquarters division. The head of the intelligence directorate is the performance "rating official" for only four people at the Bureau—three special assistants and the Assistant Director of the office.[70] In turn, the Assis-

tant Director rates only three people outside of the Directorate of Intelligence.[71] And unlike the Assistant Directors in the Counterintelligence, Counterterrorism, and Criminal Divisions, the Assistant Director of the Directorate of Intelligence does not rate the heads of the 56 field offices,[72] nor does anyone in the Directorate of Intelligence have any personnel rating authority (direct or indirect) over the Field Intelligence Groups or their supervisors.[73] At best, the intelligence directorate exercises a series of broken lines of authority over the Bureau's national security functions. In turn, these broken lines also represent a broken chain of influence for the Director of National Intelligence.

"Intelligence Elements" of the FBI

The DNI has one more power over the FBI's intelligence activities—in theory, at any rate. The new intelligence act empowers the DNI to lead the Intelligence Community, which it defines as including the FBI's "intelligence elements."[74] What are those elements? Neither the statute nor the FBI has defined the term. In our view, those elements should include the Bureau's principal intelligence-gathering units—the Counterterrrorism and Counterintelligence Divisions, as well as the intelligence directorate itself. Once again, because this issue has not been resolved, it is not clear that the FBI's national security-related divisions will in fact be subject to effective oversight and coordination by the DNI.

In reforming its intelligence capabilities since September 11, the FBI opted not to fundamentally reorganize its existing operational structure. Thus while the Bureau has significantly improved (and certainly has further plans to improve) many of its intelligence *capabilities*, it has not integrated these capabilities to ensure that national intelligence requirements and strategic analysis drive counterterrorism, counterintelligence, and foreign intelligence operations, investigations, and collection. And in our view, whether the DNI and the FBI will be able to direct those resources effectively and in meaningful coordination with the rest of the Intelligence Community remains in question so long as the FBI's primary national security components answer to different chains of authority outside of the DNI's aegis.

Realigning the FBI's Intelligence Elements

Recommendation 1

To ensure that the FBI's *intelligence elements* are responsive to the Director of National Intelligence, and to capitalize on the FBI's progress, we recommend the creation of a new National Security Service within the FBI under a single Executive Assistant Director. This service would include the Bureau's Counterterrorism and Counterintelligence Divisions and the Directorate of Intelligence. The service would be subject to the coordination and budget authorities of the DNI as well as to the same Attorney General authorities that apply to other Bureau divisions.

To resolve these issues of coordination and authority and to facilitate further reform, we propose a National Security Service within the FBI. This service would include the FBI's Counterintelligence and Counterterrorism Divisions, as well as its Directorate of Intelligence.

The creation of such a service would bring the FBI's operational divisions with national security responsibilities under the DNI's authority. The service would account for all of the FBI's National Intelligence Program-funded resources, thereby giving the DNI effective budget control as well. The service would be led by an Executive Assistant Director. In order to preserve the intelligence reform act's intent that the DNI have a say in the appointment of the FBI's top intelligence official, this individual would serve in the role of the Executive Assistant Director for Intelligence.

Because of the strength of the FBI's field offices, some link between the head of the service and certain field offices is also needed. For example, the National Security Service could have authority to approve and evaluate Special Agents in Charge of the 15 field offices that have an official foreign diplomatic presence. The service should also have inspection authority to evaluate the work of FBI's field offices. Through these evaluation and appointment authorities, the headquarters elements of the service (and through them, the DNI) would have a lever to ensure that the FBI is accountable for fulfilling national intelligence requirements through its investigatory, operational, and collection capabilities.

Recognizing the danger that field offices may drain National Security Service resources for more immediate law enforcement needs, we recommend the development of a process to prevent excessive diversion of the service's resources. This is not to say that National Security Service resources will never be re-allocated to other missions, but that they should be re-allocated or detailed to other divisions only temporarily, and only with the permission of the head of the National Security Service, under procedures agreed upon by the DNI.

Like the 9/11 Commission, we considered and rejected the creation of a separate agency devoted entirely to internal security without any law enforcement powers.[75] The FBI's hybrid nature is one of its strengths. In today's world of transnational threats, the line between "criminal activity" and "national security information" is increasingly blurred, as is well-illustrated by the use of illegal drug proceeds to fund terrorist activity. The FBI can quickly bring criminal justice tools, such as search warrants, to bear in its national security mission. In addition, the FBI's criminal justice role demands everyday contact with state and local officials—contact that is invaluable for obtaining information relevant to national security.

We believe it is critical that the National Security Service remain within the FBI. Personnel in the service would take advantage of its specialized career options, but agents in the service would go through law enforcement training along with their counterparts in the FBI's criminal divisions. Agents could laterally transfer between the service and the FBI's other divisions mid-career.

Because the National Security Service will remain part of the FBI, analysts will continue to work in the headquarters components of the non-service divisions and on criminal cases in the field offices. The FBI will continue to hire all of its personnel through a single office; its information technology and information sharing infrastructure will remain combined; and the support service functions will still serve the entire Bureau.

Ensuring continuing coordination between the FBI's two halves is critical for at least two reasons: such coordination is necessary to optimize the FBI's performance in both national security and criminal investigations, and—equally important—it will help ensure continued attention to civil liberties and legal limits on the power of government to intrude into the lives of citizens. Of course, all activities in the National Security Service would be performed consistent with the Attorney General Guidelines for national security investi-

gations and foreign intelligence collection, as well as under Department of Justice and Congressional oversight.

As long as the Bureau continues to expose Special Agents to a tour of criminal work, as it should, its agents will have experience in criminal justice matters and continue to be extensively trained to uphold the Constitution and protect civil liberties. Working in the criminal justice environment sensitizes agents to civil liberties limits on a daily basis, through regular contact with Department of Justice attorneys as well as the courts. The Bureau's national security and criminal justice components can and must continue to work together.

If that is done, we see no civil liberties protections to be gained by requiring that personnel work separately in the Counterterrorism or Counterintelligence Divisions rather than a National Security Service that combines these divisions. In fact, civil liberties protections would if anything be increased if, as we suggest, investigations of purely domestic terrorism were assigned to the FBI's Criminal Division. There is no civil liberties reason to insulate National Intelligence Program funds from the oversight of the DNI. Nor do we believe that civil liberties are diluted if the head of the National Security Service sets intelligence priorities or performs personnel evaluations of Special Agents in Charge.

In short, without creating walls between the FBI's national security and criminal components, the National Security Service would establish a single focal point for the Bureau's national security mission and a series of direct lines connecting the DNI to the national security elements at FBI headquarters and in the field. The proposed service would provide a more defined and prestigious career track for agents focused on national security. It would also enhance the Bureau's intelligence capabilities, providing strategic analysis, asset validation, intelligence career planning, training, and strategic targeting for the FBI's overall national security mission—functions that are now scattered and, in many cases, undeveloped. A National Security Service would protect national security intelligence resources, demand real accountability, and ensure that intelligence requirements are met—all without fundamentally changing the structure or nature of the FBI's 56 field offices that are the hallmark of the organization. In the field offices agents will continue to do both intelligence and criminal work; collectors and analysts will continue to work side by side.

Despite all of these advantages to creating a National Security Service within the FBI, we are compelled to add a note of caution—the same that was eloquently sounded by the 9/11 Commission:

> We have found that in the past the Bureau has announced its willingness to reform and restructure itself to address transnational security threats, but has fallen short—failing to effect the necessary institutional and cultural changes organization-wide. We want to ensure that this does not happen again.[76]

Our recommendations attempt to effect this necessary institutional change, and to instill a culture that is truly consistent with the demands of national security intelligence operations. In our view, while the FBI has made steps in the right direction since September 11, it still has many miles to travel. Reform will require enormous commitment and effort within the FBI, as well as sustained outside coordination and oversight. And despite the many benefits associated with having a combined law enforcement and intelligence agency, we recommend that policymakers re-evaluate the wisdom of creating a separate agency—an equivalent to the British "MI-5"—dedicated to intelligence collection in the United States should there be a continued failure to institute the reforms necessary to transform the FBI into the intelligence organization it must become.

ENDING THE TURF WAR BETWEEN THE FBI AND THE CIA

Recommendation 2

The DNI should ensure that there are effective mechanisms for preventing conflicts and encouraging coordination among intelligence agencies in the United States.

Both CIA and the FBI have long had responsibilities for foreign intelligence collection in the United States, subject in both cases to Attorney General oversight.[77] If anything, the need for continued activity on the part of both agencies will only increase. Valuable foreign assets and lucrative targets can come

and go across our borders practically as they please. The Intelligence Community must be as agile and flexible as their target's travel plans.

The past four years have witnessed many instances of exemplary and ongoing cooperation between CIA and FBI; the two agencies have, among other achievements, increased joint operations and successfully worked together against several hard target countries.[78] But clashes have become all too common as well, particularly in the context of intelligence gathered in the United States. When sources provide information to both agencies, the FBI complains that conflicting or duplicative reports go up the chain, causing circular or otherwise misleading streams of reporting.[79] In response, CIA claims that FBI headquarters is more concerned about credit for intelligence production than the quality of its reporting.[80] If the agencies' fight were limited to disputes about who gets credit for intelligence reports, it would be far less alarming. Unfortunately, it extends beyond headquarters and into the field, where lives are at stake.

Overseas, lack of cooperation between CIA and FBI has resulted in clashes over interaction with foreign liaison services and over coordination of other activities.[81] Both agencies agree that lack of coordination has jeopardized ongoing intelligence activities.[82]

Moreover, officials from CIA's Counterterrorist Center told us that they have difficulty tracking and obtaining information about terrorist cases after they hand them off to the FBI—as they must do when the focus of a case shifts from overseas to the territorial United States.[83] The failure of CIA and FBI to cooperate and share information adequately on such cases could potentially create a gap in the coverage of these threats, like the one the September 11 attack plotters were able to exploit.[84]

These conflicts between agencies that should regard each other as compatriots signal the need for a strong Intelligence Community leader with effective, acknowledged authority over both CIA and FBI—for a DNI, in fact.

In our view, the primary source of friction concerns the FBI's desire to expand its current authorities relative to intelligence activities and production within the United States. The FBI is, of course, the largest and most active collector of intelligence inside the United States, but the CIA has long had officers collecting intelligence in the United States as well. In December 2004, the FBI pro-

posed a new Memorandum of Understanding to govern intelligence coordination between the FBI and CIA.[85] The FBI's proposed guidelines exhibit the Bureau's desire for new controls over other agencies' activities and intelligence production in the United States. At least some in CIA have interpreted the FBI's recent initiatives as an attempt by the Bureau to gain control over CIA operations in the United States.[86]

The Commission asked the FBI to identify significant risks or problems associated with continuing to allow CIA to carry out non-intrusive foreign intelligence activities inside the United States under existing guidelines and authorities. The Bureau responded that lack of coordination has occasionally resulted in different agencies identifying the same targets, recruiting the same sources, and disseminating circular reporting.[87] The FBI's draft Memorandum of Understanding appears, however, to be an extreme reaction to these concerns. While we cannot discuss the details of the FBI's proposed Memorandum in an unclassified report, we believe that the Bureau's proposal establishes procedures that are overly burdensome and counterproductive to effective intelligence gathering.

The FBI's generalized statements about the need for coordination do not justify the kinds of restraints that it is seeking to impose. To the extent that the FBI is seeking to impose constraints on the CIA that parallel those that the CIA imposes on FBI operations abroad, the analogy is misguided. Foreign operations often occur in a hostile environment where lack of coordination can be fatal and U.S. embassies provide a logical focal point for coordinating intelligence activities in that country. Neither is true of activities inside the United States.

In claiming new territory, the FBI has argued that it is too hard to define assets or to place them in counterintelligence, counterterrorism, or foreign intelligence "boxes."[88] We think this is all the more reason to have a fluid system for coordination—where both agencies are involved in the collection of foreign intelligence in the United States and conflicts are resolved by the DNI (or the Attorney General if it is a question of what U.S. law permits). Only increased cooperation, better procedures to accomplish it, and responsiveness to strong national leadership will help to resolve conflicts when they occur. The days of negotiated treaties among sovereign intelligence agencies are over, or should be. This dispute should be resolved by the DNI and monitored to ensure consistent improvement.

Bringing the FBI's national security elements under the direction of the DNI will be a significant step towards achieving this increased agility and simultaneously ensuring that the Intelligence Community agencies act in concert against foreign intelligence targets. In addition to developing effective mechanisms for coordination, the DNI will need authority to arbitrate between agencies in instances of conflict, an authority the DNI will only have if the FBI becomes a fully responsive and accountable member of the Intelligence Community.

A final, and critical, point: in exercising this authority, we expect the DNI to require scrupulous adherence to Attorney General Guidelines designed to protect civil liberties. Nothing in our call for greater coordination between the FBI and CIA is meant to alter *in any way* existing civil liberties protections. The best way to protect civil liberties is not by favoring one agency over another but by ensuring that every agency adheres to the law. That is the purpose of the Attorney General's Guidelines, which establish rules both for FBI national security investigations and foreign intelligence collection,[89] and for the CIA's foreign intelligence and counterintelligence activities in the United States.[90] The Guidelines strictly delineate the manner in which each agency can conduct operations, providing the clarity necessary to protect civil liberties. Perhaps most importantly, both sets of Guidelines make clear that the CIA must turn to the FBI, which must in turn obtain either Justice Department or court approval, for *any* remotely invasive or non-consensual activity, such as searches, electronic surveillance, or non-consensual interviews within the United States.[91] Coordination will not change any of these rules; indeed, giving the DNI coordinating authority without revising the Guidelines will likely enhance the protection of civil liberties, for it will ensure that all domestic collection is carefully supervised, coordinated, and directed.

THE DEPARTMENT OF JUSTICE: THE REMAINING REORGANIZATION

Recommendation 3

The Department of Justice's primary national security elements—the Office of Intelligence Policy and Review, and the Counterterrorism and Counterespionage sections—should be placed under a new Assistant Attorney General for National Security.

In the wake of September 11, much criticism rightly focused on legal and procedural impediments to information sharing—the proverbial "wall"—between U.S. law enforcement agents and intelligence officers. As a result, all three branches of government dismantled the dividing elements between these two functions. Major changes were made at the CIA, FBI, and Department of Homeland Security. The core organization of the Justice Department, however, did not change at all.

The Justice Department's three primary national security components are located in different divisions, with no individual below the Deputy Attorney General who can supervise all three. The Office of Intelligence Policy and Review (OIPR) is responsible for FISA requests, representing the Department of Justice on intelligence-related committees, and advising the Attorney General on "all matters relating to the national security activities."[92] It is independent of any division and reports directly to the Deputy Attorney General. In contrast, both the Counterterrorism and Counterespionage sections are located in the Criminal Division, but they each report to two *different* Deputy Assistant Attorneys General. If there is method to this madness, neither we, nor any other official with whom we spoke, could identify it.

There is reason to believe that this awkward (and outdated) organizational scheme has created problems between the Justice Department and the Intelligence Community. In our classified report we describe one such problem that cannot be discussed in our unclassified report.

We believe that bringing the Office of Intelligence Policy and Review closer to its operational counterparts like the Counterespionage and Counterterrorism sections would give the office better insight into actual intelligence practices and make it better attuned to operational needs. Attorneys in the Counterterrorism and Counterespionage sections routinely work alongside FBI agents and other intelligence officers. By contrast, OIPR is largely viewed within the Department as an "assembly line operation not requiring any special grounding in the facts of a particular matter."[93] OIPR's job is to process and adjudicate FISA requests—not to follow a case from start to completion. One of the advantages of placing all three national security components under a single Assistant Attorney General is that they will see themselves as acting in concert to serve a common mission.[94]

In our view, a more effective construct would place an Assistant Attorney General for National Security in charge of all three national security elements (OIPR, Counterespionage, and Counterterrorism).[95] This Assistant Attorney General would serve as a single focal point on all national security matters. The Assistant Attorney General would be responsible for reviewing FISA decisions and determining what more can be done to synthesize intelligence and law enforcement investigations. In an era when it is becoming increasingly incumbent upon organizations like the FBI to balance both their law enforcement and intelligence responsibilities, more thoughtful, innovative, and constructive legal guidance is in high demand.

A further possibility would be to create a new Associate Attorney General position that was responsible for both the Criminal Division and our recommended National Security Division.[96] This construct has the advantage of ensuring that criminal and national security measures are "merged" prior to reaching the Deputy Attorney General, who is responsible for operations within the entire Department of Justice extending far beyond criminal and national security matters. This structure also has the added benefit of providing the Justice Department with management levels more closely aligned with those of other departments (*i.e.*, the cabinet Secretary, a Deputy Secretary, and Under Secretaries).

Furthermore, this construct would align the Justice Department's national security elements with the Intelligence Community. It would create a structure that is parallel to the one proposed for the FBI, and would highlight that Department of Justice attorneys are not just there to advise the Bureau if a matter becomes a criminal investigation. We believe this integration would make Justice more responsive to the FBI's needs and perhaps better able to allocate resources to the national security mission in general.

THE DEPARTMENT OF HOMELAND SECURITY: MORE WALLS TO BREACH

The Department of Homeland Security is the primary repository for information about what passes in and out of the country—a critical player safeguarding the United States from nuclear, biological, or chemical attack. Yet since its inception Homeland Security has faced immense challenges in collecting information efficiently, making it available to analysts and users both inside

and outside the department, and bringing intelligence support to law enforcement and first responders who seek to act on such information.

Although we have included Homeland Security in our discussion of intelligence collection within the United States, we have not completed a detailed study of the Department's current capabilities. We will therefore make only one formal recommendation with respect to Homeland Security. Nonetheless, it is plain that Homeland Security faces challenges in all four of the roles it plays in the Intelligence Community—as collector, analyst, disseminator, and customer.

The Department of Homeland Security has no shortage of intelligence collectors. With 22 agencies, Homeland Security commands more than 180,000 personnel from the U.S. Coast Guard, Customs and Border Protection, Secret Service, Immigration and Customs Enforcement (ICE), Transportation Security Administration, and Office of Infrastructure Protection.[97] ICE has more than 3,000 employees.[98] ICE collects reams of data on foreigners entering the United States and manages the Student and Exchange Visitor Information System database, which includes information on foreign students studying in the United States. However, whether agencies like ICE are equipped to make this information available to the Intelligence Community in useable form remains unclear. ICE officials explained that they would not give other agencies unfettered access to their databases (despite those agencies' wishes) because of unspecified legal constraints.[99] We find this September 10th approach to information sharing troubling; it deserves careful scrutiny from the DNI and the new Secretary of Homeland Security, to ensure there is full information sharing consistent with intelligence needs and valid civil liberties concerns.

A critical Homeland Security function is disseminating threat information to law enforcement and other officials at the federal, state, local, and tribal level. The Department of Homeland Security currently faces many difficulties in this regard. According to one Homeland Security official, local law enforcement officials are currently "shotgunned" by the information flow coming from a variety of federal sources, and confused as to who has the lead in supporting their information and intelligence needs.[100] Senior officials at Homeland Security emphasize that the process of declassifying information takes too long and frequently prevents the department from quickly sharing concrete, actionable information with law enforcement.[101] Instead, law enforcement officials often receive a steady steam of vague

threat reporting, unsupported by adequate sourcing, and incapable of serving as a basis for action.

Homeland Security's problems with sharing national security information do not end there. Like many other intelligence organizations, Department of Homeland Security officials expressed concerns about the lack of procedures for sharing intelligence across agencies. As an example, Homeland Security officials have expressed concern that they have no mechanism for getting answers to "hot questions" they pose to the FBI and the National Counterterrorism Center.[102] Some of the obstacles to interagency collaboration are even more basic. As one senior Homeland Security official in the Information Analysis section remarked about the FBI, "I still can't send them an e-mail, and they can't send one back."[103] Finally, in a variation on a familiar theme, some law enforcement agents at Homeland Security have expressed unwillingness to share operational information out of concern that other agencies might seek to "steal" their cases.[104]

Recommendation 4

The Secretary of Homeland Security should rescind Treasury Order 113-01 as it applies to Department of Homeland Security elements.

Homeland Security's approach to information sharing unfortunately draws sustenance from rules that Immigration and Customs Enforcement inherited from the Treasury Department. ICE currently operates under an old Treasury order (T.O. 113-01) regarding requests for assistance from the Intelligence Community.[105] Established in the wake of the Iran-Contra affair, this order requires that all requests by the Intelligence Community for assistance be reduced to writing and submitted for approval to the Secretary or Deputy Secretary of the Treasury. The order provides an exception only for "routine exchange between the Intelligence Community and the Department of the Treasury of substantive intelligence information and recurring reports."[106] It leaves the interpretation of what constitutes a "routine" exchange up to the head of the agency involved. The order apparently applies to all information sharing agreements between former Treasury elements of Homeland Security and the Intelligence Community, since they are not considered "routine."[107] When the Department of Homeland Security was created and Immigrations and Customs Enforcement was transferred to its jurisdiction, the order

remained in effect, although oversight was shifted to the Under Secretary for Border and Transportation Security.[108]

We find it highly disappointing that such a barrier to communication between law enforcement and intelligence agencies has survived in a department created to avoid the mistakes and miscommunication that led to the September 11 attacks. It should be rescinded, not extended. The default policy for personnel within Homeland Security component agencies should be to cooperate with requests for assistance and information sharing coming from the Intelligence Community, not to refer such requests to a lengthy and bureaucratic process practically designed to deter collaboration. We strongly recommend that the Secretary of Homeland Security promptly rescind Treasury Order 113-01 and replace it with a new order that ensures greater information sharing and collaboration between all entities of Homeland Security and the Intelligence Community. Similarly, we believe that the Department of the Treasury should evaluate whether its successor to Treasury Order 113-01 (Treasury Order 105-18) should be modified to effect smoother cooperation within the Intelligence Community.

ENDNOTES

[1] The FBI refers to itself in these terms. According to the FBI, "now that the Intelligence Program is established and developing, we are turning to the next stage of transforming the Bureau into an intelligence agency." FBI, *The FBI's Counterterrorism Program Since September 2001, Report to the National Commission on Terrorist Attacks upon the United States* (April 14, 2004) at p. 31. Director Mueller also refers to the FBI as "both a law enforcement and an intelligence agency." *Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Before the United States Senate Committee on the Judiciary* (May 20, 2004).

[2] Interview with U.S. Immigration and Customs Enforcement official (Feb. 28, 2005).

[3] According to Director Mueller, in 2004, 30 percent of new hires had accounting, law enforcement, and military backgrounds. Interview with Robert Muller, FBI Director (Oct. 20, 2004).

[4] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004) at p. 425 (hereinafter "9/11 Commission Report").

[5] As a result of the FBI's strategic plan of 1998, the Bureau created an Office of Intelligence. One year later, in November 1999, the FBI created an Investigative Services Division that subsumed the Office of Intelligence and was designed to "house a new Information, Analysis and Assessments Branch." FBI, *Press Release* (Nov. 11, 1999). According to a 1999 FBI press release, the aim of the Investigative Services Division was to extract information from case files "and other existing sources to identify future trends and means of preventing crime and threats to national security. The FBI intends to increase its reliance on information analysts and to devote additional efforts to recruiting highly qualified persons to perform this function." *Id.*

[6] According to a 9/11 Commission staff statement, at the time that the Investigative Services Division was set up, an internal FBI review "found that 66 percent of the bureau's analysts were not qualified to perform analytical duties….The new division did not succeed. FBI officials told us that it did not receive sufficient resources, and there was ongoing resistance to its creation from senior managers in the FBI's operational divisions. Those managers feared losing control. They feared losing resources. They feared they would be unable to get the assistance they wanted from the new division's analysts." 9/11 Commission Staff Statement # 9, *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11* (April 13, 2005) at pp. 5-6; *see also* Alfred Cumming and Todd Masse, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress* (CRS Report RL 32336) (updated Aug. 4, 2004) at p. 58.

[7] Interview with FBI Directorate of Intelligence official (Jan. 19, 2005).

[8] Interview with FBI Special Agent in Charge (Dec. 8, 2004) (using this example to describe how the demands on field offices may vary, in part, according to location).

[9] *Id.*

[10] Simply in quantitative terms, the majority of FBI's reporting comes in the form of Intelligence Information Reports (IIRs), unfinished intelligence products. In recent years the Bureau has dramatically increased the number of IIRs it produces. Further details are provided in our classified report that we cannot reference here.

[11] FBI Directorate of Intelligence, *Report to the President of the United States: Comprehensive Plan for the FBI Intelligence Program with Performance Measures* (Feb. 16, 2005) at p. 28

(hereinafter "FBI, Comprehensive Plan").

[12] FBI Directorate of Intelligence, *Cincinnati Division Field Intelligence Group On-Site Review* (Oct. 13, 2004) at p. 6.

[13] National Academy of Public Administration, *Transforming the FBI: Progress and Challenges* (Jan. 2005) at p. xv. The report notes that "[i]n-depth strategic collection and analysis efforts tend to be deferred at the FBI." *Id.*

[14] Further details are provided in our classified report that we cannot reference here. In Fiscal Year 2004, the FBI published 250 Intelligence Assessments. FBI, *Office of Intelligence Response to Request # 15* (Jan. 5, 2005).

[15] Interview with FBI official (Oct. 22, 2004).

[16] 9/11 Commission Staff Statement # 9, *Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11* (April 13, 2004) at p. 9.

[17] FBI Directorate of Intelligence, *Office of Intelligence On-Site Review of Field Intelligence Groups* (Sept. 10, 2004) at p. 6.

[18] Currently 25 percent of the Bureau's analytic cadre has an advanced degree. Interview with FBI Directorate of Intelligence official (Oct. 18, 2004). In comparison, 60 percent of analysts in CIA's Directorate of Intelligence have an advanced degree. Interview with CIA Directorate of Intelligence Human Resources official (Jan. 10, 2005).

[19] The failure to communicate fabrication notices properly was, specifically, a problem for Defense HUMINT Service. Chapter One (Iraq).

[20] Interview with FBI counterintelligence official (Feb. 18, 2005).

[21] *Id.*

[22] *See, e.g.*, Interview with FBI Field Intelligence Group official (Feb. 3, 2005).

[23] Interview with FBI official (Jan. 24, 2005).

[24] Senator Shelby wrote, "The FBI has never taken information technology very seriously, and has found itself left with an entirely obsolete information technology infrastructure that is wholly inadequate to the FBI's current operational needs, much less to the task of supporting sophisticated all-source intelligence fusion and analysis." Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence, *September 11 and the Imperative of Reform in the U.S. Intelligence Community* (Dec. 10, 2002) at p. 72.

[25] *Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Before the Untied States Senate Committee on the Judiciary* (May 20, 2004) ("Our goal is to deliver Virtual Case File capabilities by the end of this year").

[26] National Research Council of the National Academies, James C. McGroddy and Herbert S. Lin (Eds.), *A Review of the FBI's Trilogy Information Technology Modernization Program* (2004) at pp. 3-4, 26.

[27] Interview with FBI official (Dec. 15, 2004).

[28] FBI Directorate of Intelligence, *Response to Commission FBI Request # 15* (Jan. 5, 2005).

[29] The FBI has a total of 12,254 Special Agents. Interview with FBI Directorate of Intelligence official (Jan. 19, 2005).

[30] Executive Order No. 12333 (Dec. 4, 1981) at § 1.14(a).

[31] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-

458 (hereinafter "IRTPA").

[32] *Id*.

[33] *Id.*

[34] *See, e.g.,* Interview with FBI official (March 7, 2005).

[35] *See, e.g.,* Interview with Office of Management and Budget officials (Feb. 8, 2005). While the FBI's NIP dollars are *appropriated* through the House Subcommittee on Science, State, Justice, and Commerce, and Related Agencies and the Senate Subcommittee on Commerce, Justice, and Science, these dollars are *identified* as part of the NIP budget.

[36] FBI, *National Foreign Intelligence Program FY 2005 President's Request* (Jan. 27, 2004).

[37] Interview with Office of Management and Budget officials (Feb. 8, 2005).

[38] IRTPA at § 1014(b)(2)(H).

[39] *Id*. at § 2001(f); *see also* 9/11 Commission Report at p. 426 (recommending that the FBI "align its budget structure according to its four main programs…to ensure better transparency on program costs, management of resources, and protection of the intelligence program").

[40] FBI, Comprehensive Plan at p. 9.

[41] *Id.* at p. 10 (noting that the FY 2005 Intelligence Decision Unit Budget is $819,108,658 and that 39 percent of the Intelligence Decision Unit Budget goes to the Directorate of Intelligence, Criminal program, and Administrative Support combined). The Directorate of Intelligence, Criminal Division, and Administrative Support are not included in the National Intelligence Program budget. FBI, *National Foreign Intelligence Program FY 2005 President's Request* (Jan. 27, 2004); *see also* Interview with Office of Management and Budget official (March 16, 2005).

[42] FBI, Comprehensive Plan at p. 9.

[43] Interview with Office of Management and Budget official (March 8, 2005).

[44] FBI, Comprehensive Plan at p. 10.

[45] *Id.*

[46] Interview with Office of Management and Budget official (March 8, 2005) (suggesting, nevertheless, that several of the Executive Assistant Director's various specific budgetary authorities relative to the Intelligence Decision Unit may be currently undetermined). FBI states that the only individual with budget execution authority is the Director of the FBI. Interview with FBI official (March 7, 2005).

[47] FBI, Comprehensive Plan at p. 10.

[48] IRTPA at § 1014.

[49] *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* (May 30, 2002) at p. ii.

[50] IRTPA at § 1014(b)(2)(H).

[51] *Id.* at § 2002(c).

[52] *Id.* at § 2002(c)(1) & (3).

[53] FBI, Comprehensive Plan at p. 15. The Directorate of Intelligence indicates that field intelligence operations constitute the process of "identify[ing]" intelligence gaps, "lev[ying]" requirements as "tasks," providing "support" to the intelligence cycle, "conduct[ing] intelli-

gence assessments" and "know[ing] and report[ing] the scope and extent of [Field Office] collection capabilities." *Id.* at pp. 3-4. In some cases, Field Intelligence Groups are like other FBI field office components, or "squads" (*e.g.*, counterterrorism, counterintelligence, criminal, and cybercrime). In other cases, they are more nascent and embedded in existing operational squads. FBI Directorate of Intelligence, *FBI Field Office Intelligence Operations: Concept of Operations* (Aug. 2003) at p. 2.

[54] FBI, *Response to Commission FBI Request # 16-1 through 16-10* (Feb. 3, 2005) at pp. 3-4.

[55] Interview with FBI Directorate of Intelligence officials (Nov. 18, 2004).

[56] Interview with FBI official (Jan. 18, 2005); Interview with FBI Field Intelligence Group official (Feb. 3, 2005).

[57] FBI, Directorate of Intelligence, *Columbia Division Field Intelligence Group On-Site Review* (Jan. 3, 2005) at p. 12.

[58] 9/11 Commission Report at p. 423.

[59] Interview with Directorate of Intelligence official (Jan. 19, 2005). In contrast, the FBI's operational divisions are explicitly given authorities to task field offices as well as initiate and terminate cases.

[60] FBI, Comprehensive Plan at p. 15.

[61] As defined, the Field Intelligence Groups do not have authorities to drive counterintelligence and counterterrorism investigations, collections, and operations. Interview with Directorate of Intelligence official (March 8, 2005).

[62] FBI Directorate of Intelligence, *Response to Commission FBI Request # 15* (Jan. 5, 2005).

[63] FBI Directorate of Intelligence, *Response to Commission FBI Request # 10* (Sept. 30, 2004).

[64] IRTPA at § 2002(c)(6).

[65] Interview with Directorate of Intelligence official (Jan. 19, 2005). As noted earlier, the Bureau has stated that it plans on adding a strategic analysis unit to the Directorate of Intelligence. However, it is not clear whether this unit will conduct strategic analysis or instead provide guidance for the field offices on how to produce such reporting. FBI, Comprehensive Plan at p. 28.

[66] Interview with Directorate of Intelligence official (Jan. 19, 2005).

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] They are a Deputy Assistant Director in the Counterterrorism Division (an evaluation that is then reviewed by the head of the Counterterrorism Division) and two section chiefs in the Criminal and Counterintelligence Divisions. In the first case, the Deputy Assistant Director is rated by one component of the FBI and reviewed by another. Even more peculiar, while the Directorate of Intelligence has rating authority for a Deputy Assistant Director in Counterterrorism, in the Criminal and Counterintelligence Divisions the Assistant Director of the Directorate of Intelligence is the rating official for a Section Chief. *Id.*

[72] Interview with Directorate of Intelligence official (March 8, 2005). Although the Assistant Director of the Directorate of Intelligence does not rate the heads of the field offices like the Assistant Directors in these other divisions, the Assistant Director does provide *input* into these evaluations. *Id.* The Assistant Directors in FBI's Counterintelligence, Counterterrorism, and Criminal Divisions rate the heads of FBI's 56 field offices on a rotating basis.

[73] *Id*.

[74] IRTPA at § 1073.

[75] This was one proposal that the 9/11 Commission considered. According to the 9/11 Commission Report, "we have considered proposals for a new agency dedicated to intelligence collection in the United States….We do not recommend the creation of a new domestic intelligence agency. It is not needed if our other recommendations are adopted—to establish a strong national intelligence center, part of the NCTC, that will oversee counterterrorism intelligence work, foreign and domestic, and to create a National Intelligence Director who can set and enforce standards for the collection, processing, and reporting of information." 9/11 Commission Report at p. 423.

[76] *Id.* at p. 425.

[77] According to Executive Order 12333, CIA shall "[c]ollect, produce, and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable. The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General." Executive Order 12333 at § 1.8(a). The FBI shall "[c]onduct within the United States, when requested by officials of the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Security Agency, to support communications security activities of the United States Government; produce and disseminate foreign intelligence and counterintelligence." *Id*. at § 1.14 (c)(d). According to the Intelligence Reform and Terrorism Prevention Act of 2004, the CIA shall "provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community authorized to undertake such collection." *Id.* at § 1011. The act is silent on CIA's domestic responsibilities for foreign intelligence.

[78] Classified CIA report.

[79] Interview with senior FBI officials (Dec. 22, 2005).

[80] Classified CIA report.

[81] *Id.*

[82] *Id*.; FBI, *Response to Commission FBI Request # 16* (Feb. 3, 2005).

[83] Interview with Counterterrorist Center WMD Unit official (Oct. 22, 2004).

[84] 9/11 Commission Report at p. 263.

[85] FBI, *Draft Memorandum of Understanding Between the Central Intelligence Agency and the Federal Bureau of Investigation Concerning the Coordination of CIA Activities in the United States and FBI Activities Abroad* (Dec. 13, 2004) (hereinafter "FBI Draft MOU").

[86] Classified CIA report.

[87] FBI, *Response to Commission FBI Request # 16* (Feb. 3, 2005).

[88] Interview with FBI official (Dec. 22, 2004).

[89] *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (Oct. 31, 2003).

[90] CIA, *Guidance for CIA Activities Within the United States* (HR 7-1) (Dec. 23, 1987) at Annex B.

[91] *Id.* In a submission to the Commission, the Center for National Security Studies expressed serious concerns about the degree to which the CIA's domestic activities were regulated. *See generally* Letter to the Commission from Kate Martin, Center for National Security Studies, *Re: Intelligence Activities in the U.S.: Current Proposals' Risks to Civil Liberties* (Feb. 16, 2005). More specifically, the Center recommended that the CIA's activities "be carried out pursuant to guidelines that are written by the Attorney General." *Id.* at p. 8. As we have just noted, this is already the case. And although we cannot, due to classification, discuss details of the current Attorney General-approved guidelines that regulate the CIA's activities in the United States, we can say that the guidelines are highly detailed and significantly *more* restrictive than those applicable to the FBI. Furthermore, the Department of Defense is subject to similar Attorney General guidelines for Defense Department intelligence activities affecting U.S. persons. Department of Defense, DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* (Dec. 1982).

[92] Department of Justice, *Office of Intelligence Policy and Review* (Dec. 12, 2003) *available at* http://www.usdoj.gov/oipr (accessed March 12, 2005).

[93] *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* (May 2000) at p. 767 (hereinafter "Bellows Report").

[94] The Bellows Report identifies a further reason to have a single individual below the Deputy Attorney General to supervise OIPR: the need to have a single individual who is knowledgeable about FISA to review FISA applications that are rejected by OIPR. *Id.* at pp. 767-768. The lack of such an individual in the Wen Ho Lee investigation caused serious problems. An Assistant Attorney General for National Security would fit the bill perfectly.

[95] Prior to the Church and Pike investigations, the Department of Justice had such a unit. Since September 11, Justice officials have considered, but not pressed forward, with such a reorganization. Interview with former Assistant Attorney General (Nov. 30, 2004).

[96] The Department currently has a single Associate Attorney General who supervises the Civil Rights, Antitrust, Tax, Civil, and Environmental Divisions, along with several other smaller offices. Department of Justice Organizational Chart (July 14, 2003). There is no such intermediary between the Criminal Division (and several other offices) and the Deputy Attorney General.

[97] Interview with Department of Homeland Security Information Analysis and Infrastructure Protection official (Oct. 7, 2004).

[98] *Id.*

[99] Interview with Immigration and Customs Enforcement officials (Sept. 27, 2004).

[100] Interview with Department of Homeland Security Office of State and Local Coordination official (Dec. 9, 2004).

[101] Interview with Department of Homeland Security Information Analysis and Infrastructure Protection official (Jan. 6, 2005).

[102] Interview with Department of Homeland Security Information Analysis and Infrastruc-

ture Protection official (Dec. 17, 2004)

[103] Interview with Department of Homeland Security Information Analysis and Infrastructure Protection official (Oct. 7, 2004).

[104] Interview with Department of Homeland Security official (Jan. 6, 2005).

[105] Treasury Order 113-01 (Dec. 19, 2002) (superseding provision of same order).

[106] *Id.* at § 4.

[107] Interview with Department of Homeland Security Office of General Counsel official (March 2, 2005).

[108] Homeland Security Act of 2002 § 1512, Pub. L. No 107-296 (providing that the orders of an agency transferred to DHS shall remain in effect according to their terms until lawfully amended, superseded, or terminated).

CHAPTER ELEVEN
COUNTERINTELLIGENCE

Summary & Recommendations

Even as our adversaries—and many of our "friends"—ramp up their intelligence activities against the United States, our counterintelligence efforts remain fractured, myopic, and marginally effective. Our counterintelligence philosophy and practices need dramatic change, starting with centralizing counterintelligence leadership, bringing order to bureaucratic disarray, and taking our counterintelligence fight overseas to adversaries currently safe from scrutiny.

We recommend that:

- The National Counterintelligence Executive (NCIX)—the statutory head of the U.S. counterintelligence community—become the DNI's Mission Manager for counterintelligence, providing strategic direction for the full breadth of counterintelligence activities across the government. In this role, the NCIX should also focus on increasing *technical* counterintelligence efforts across the Intelligence Community;
- The CIA create a new capability dedicated to conducting a full range of counterintelligence activities outside the United States;
- The Department of Defense's Counterintelligence Field Activity assume operational and investigative authority to coordinate and conduct counterintelligence activities throughout the Defense Department; and
- The FBI create a National Security Service that includes the Bureau's Counterintelligence Division, Counterterrorism Division, and the Directorate of Intelligence. A single Executive Assistant Director would lead the service subject to the coordination and budget authorities of the DNI.

INTRODUCTION

Enthusiasm for spying on the United States has not waned since the Cold War. Quite the reverse. The United States is almost certainly one of the top intelligence priorities for practically every government on the planet. Faced with overwhelming American military and economic might, our adversaries increasingly rely on intelligence to gain comparative advantage. A wide range of intelligence activities are used to attack systematically U.S. national security interests worldwide. Yet while our enemies are executing what amounts to a global intelligence war against the United States, we have failed to meet the challenge. U.S. counterintelligence efforts have remained fractured, myopic, and only marginally effective.

Today, we mostly wait for foreign intelligence officers to appear on our doorstep before we even take notice. The lion's share of our counterintelligence resources are expended inside the United States despite the fact that our adversaries target U.S. interests globally. Needless to say, the result is that we are extremely vulnerable outside of our borders.

The losses the United States has sustained within its borders are formidable as well. Spies such as Walker, Ames, Hanssen, and Montes have significantly weakened our intelligence and defense capabilities. Hanssen alone compromised U.S. government secrets whose cost to the nation was in the billions of dollars, not to mention the lives of numerous human sources. Our adversaries have penetrated U.S. intelligence agencies (by recruiting spies) and operations (by running double agents).[1] The theft of some our most sensitive military and technological secrets allows states like China and Russia to reap the benefits of our research and development investments.[2] And while our defense is lacking, our current counterintelligence posture also results in the loss of offensive opportunities to manipulate foreign intelligence activities to our strategic advantage.

Moreover, while stealing our secrets, our adversaries also learn *how* we spy, and how best to counter our efforts in the future, which in turn renders our remaining sources and methods even less effective and more liable to compromise and loss—a cycle of defeat that cannot be indefinitely sustained. As former Director of Central Intelligence Richard Helms once said, "No intelligence service can be more effective than its counterintelligence component for very long."[3]

We believe that U.S. counterintelligence has been plagued by a lack of policy attention and national leadership. We hope this is now coming to a close with the signing of the first national counterintelligence strategy, approved by the President on March 1, 2005. The National Counterintelligence Executive (NCIX)—the statutory head of the U.S. counterintelligence community—has characterized the new offensive counterintelligence strategy as part of the administration's policy of pre-empting threats to the security of the United States.[4]

But a new strategy alone will not do the job. As in the old—and clearly unsuccessful—approach to homeland security, U.S. counterintelligence is bureaucratically fractured, passive (*i.e.*, focusing on the defense rather than going on the offense), and too often simply ineffective.[5] But unlike homeland security, counterintelligence is still largely neglected by policymakers and the Intelligence Community. In fact, counterintelligence has generally *lost* stature since September 11, eclipsed by more immediate counterterrorism needs. While not denigrating it outright, our top policymakers and Intelligence Community management have traditionally paid lip service to counterintelligence. Until, that is, a major spy case breaks. Even then, bureaucratic defensiveness tends to win out. Senior officials have largely addressed counterintelligence issues *ad hoc*, reacting to specific intelligence losses by replacing them with new technologies or collection methods, without addressing the underlying counterintelligence problems.

We offer four recommendations to improve counterintelligence. First, that the NCIX serve as the planner, manager, and supervisor for all United States counterintelligence efforts. Second, that CIA create a new capability dedicated exclusively to attacking intelligence threats outside the United States—a capability our nation currently does not have. Third, that the Department of Defense's Counterintelligence Field Activity be given operational and investigative authority to execute department-wide counterintelligence activities. Fourth, and as discussed more fully in Chapter Ten (Intelligence at Home), that the FBI establish a National Security Service that is fully responsive to the DNI.

Counterintelligence efforts across the Intelligence Community must be better executed in support of the foreign intelligence mission. At the heart of our recommendations is the belief that an integrated and directed U.S. counterintelligence effort will take advantage of intelligence collection opportunities;

protect billions of dollars of defense and intelligence-related investments, sources, and methods; and defend our country against surprise attack.

THE COUNTERINTELLIGENCE CHALLENGE

Spies have always existed, but currently our adversaries—and many of our "friends"—are expanding and intensifying their intelligence activities against U.S. interests worldwide. They target virtually all of our nation's levers of national power—foreign policy and diplomatic strategies, strategic weapon design and capabilities, critical infrastructure components and systems, cutting edge research and technologies,[6] and information and intelligence systems.[7] Our rivals use a range of sophisticated human and technical intelligence techniques, including surveillance, spies, attempts to influence the U.S. media and policymakers, economic espionage, and wholesale technology and trade secret theft. Further, there are indications that foreign intelligence services are clandestinely positioning themselves to attack, exploit, and manipulate critical U.S. information and intelligence systems.

The United States has not sufficiently responded to the scope and scale of the foreign intelligence threat. The number of foreign agents targeting the United States is disturbing—and the majority of them are targeting U.S. interests *outside* the United States. Despite this fact, a very large proportion of U.S. counterintelligence resources are deployed inside the United States[8]—a percentage that has changed very little since the end of the Cold War.

Although we cannot discuss details at this level of classification, suffice it to say that a number of sophisticated intelligence services are aggressively targeting the United States today. These include traditional players such as China and Russia, both of whom deploy official and non-official cover officers to target American interests.[9]

But it is not only major nation states which employ aggressive intelligence services. Terrorist groups like Hizbollah and al-Qa'ida also conduct intelligence operations within the United States. The 9/11 Commission Report, for instance, detailed how the al-Qa'ida hijackers targeted U.S. sites, cased them, and otherwise engaged in classic intelligence activities such as reconnaissance.[10] According to a senior counterintelligence official at CIA, the Agency is only just beginning to understand the intelligence capabilities of terrorist organizations.[11]

Then there are adversaries who attempt to undermine the United States in more subtle ways—through covert influence and perception management efforts. A 1997 Senate investigation found that as many as six individuals with ties to the People's Republic of China sought to channel Chinese money covertly into the 1996 U.S. presidential campaign in order to influence the American political process.[12]

The sum total of these foreign intelligence efforts is striking. During the Cold War, every American national security agency—with the possible exception of the Coast Guard—was penetrated by foreign intelligence services. Moreover, in just the past 20 years CIA, FBI, NSA, DIA, NRO, and the Departments of Defense, State, and Energy have all been penetrated. Secrets stolen include nuclear weapons data, U.S. cryptographic codes and procedures, identification of U.S. intelligence sources and methods (human and technical), and war plans. Indeed, it would be difficult to exaggerate the damage that foreign intelligence penetrations have caused.

THE STATUS QUO

While our rivals have become ever more imaginative and aggressive, our own counterintelligence services remain fractured and reactive. Each U.S. counterintelligence agency pursues its own mission from its own vantage point, rather than working in concert guided by nationally-derived strategies. Our counterintelligence effort has no national focus, no systematic way to coordinate efforts at home and abroad.[13]

Among United States agencies, the FBI dominates counterintelligence within the homeland.[14] Until recently the Bureau focused its resources and operational efforts on foreign spies working out of formal diplomatic establishments—classic official-cover intelligence. The *covert* foreign intelligence presence was largely unaddressed. Today, despite bolstering its counterintelligence resources in all field offices, the FBI still has little capacity to identify, disrupt, or exploit foreign *covert* intelligence activities.[15]

Outside the United States, the CIA has primary responsibility for counterintelligence,[16] a task which, in practice, it defines very narrowly. CIA does not systematically or programmatically undertake the counterintelligence mission of protecting the equities of other U.S. government entities, nor does it mount significant, strategic offensive counterintelligence operations against rival

intelligence services. Its focus is mostly defensive; the CIA's Counterintelligence Center and the counterintelligence elements within the Directorate of Operations aim primarily to protect CIA operations.[17] CIA's current approach to counterintelligence is in contrast to its approach during the Cold War, when CIA case officers routinely targeted Warsaw Pact officials, an effort that led to a considerable number of successful counterespionage investigations.[18]

The Department of Defense, with its component counterintelligence units located within the military services, principally focuses on protecting the armed forces.[19] But no counterintelligence organization has the operational mission for the Department as a whole, leaving large swaths of unprotected areas, including highly sensitive policymaking, technology, and acquisition functions. The current system assigns each of the armed services responsibilities for counterintelligence activities in other agencies that lack their own internal capability. The services, however, do not have the range of capabilities necessary to perform this role. While the Department's Counterintelligence Field Activity (CIFA) has taken steps towards implementing a more comprehensive approach to counterintelligence, CIFA currently does not have adequate authority or resources to take on this Department-wide operational mission.[20]

As if agency-level concerns are not enough, the absence of effective and adequately empowered national counterintelligence leadership makes the situation even worse. The National Counterintelligence Executive (NCIX) is the theoretical "head" of counterintelligence,[21] but NCIX has little control over the scattered elements of U.S. counterintelligence. NCIX has only advisory budget authority, little visibility into individual agencies' counterintelligence operations, and no ability to assign operational responsibility or evaluate performance.[22] The recent intelligence reform act did not alter this situation, but it did take what we believe is a useful step—placing the NCIX in the Office of the DNI.[23]

INSTITUTIONALIZING LEADERSHIP

Recommendation 1

The National Counterintelligence Executive should become the DNI's Mission Manager for counterintelligence, providing strategic direction for the whole range of counterintelligence activities across the government.

Organizational change is not a panacea for counterintelligence, but it is necessary. Today there is no individual or office that can impose Community-wide counterintelligence reform or hold individual agencies accountable for fulfilling national counterintelligence requirements. This should change, and we believe that the obvious candidate for leadership is an empowered NCIX.

The recent intelligence reform legislation situated the NCIX in the Office of the DNI, thereby placing counterintelligence near the Intelligence Community's levers of power. To make this more than window dressing, the NCIX needs all of the DNI's authorities for counterintelligence—particularly authority over the FBI's counterintelligence operations. As the Mission Manager for counterintelligence,[24] the NCIX would build collection plans with prioritized targets and provide strategic direction to operational components. Unlike other Mission Managers, the NCIX would also be responsible for the production of strategic counterintelligence analysis.[25]

To this end, we recommend that the NCIX assume the power and the responsibility to:

- Prepare the National Intelligence Program's counterintelligence budget and approve, oversee, and evaluate how agencies execute that budget;
- Produce national counterintelligence requirements and assign operational responsibilities to agencies for meeting those requirements;
- Evaluate the effectiveness of agencies within the Intelligence Community in meeting national counterintelligence requirements;
- Direct and oversee the integration of counterintelligence tradecraft throughout the Intelligence Community;
- Establish common training and education requirements for counterintelligence officers across the Community, and expand cross-agency training;
- Identify and direct the development and deployment of new and advanced counterintelligence methodologies and technologies;
- Ensure that recommendations emerging from counterintelligence damage assessments are incorporated into agency policies and procedures;
- Deconflict and coordinate operational counterintelligence activities both inside and outside of the United States; and

- Produce *strategic* counterintelligence analysis for policymakers.

These powers would bring the NCIX on par with the other Mission Managers discussed in Chapters Six, Seven, and Eight (Leadership and Management, Collection, and Analysis).[26]

Recommendation 2

The National Counterintelligence Executive should work closely with agencies responsible for protecting U.S. information infrastructure in order to enhance the United States' technical counterintelligence capabilities.

One area we believe is especially critical for the NCIX to address is the absence of a systematic and integrated technical counterintelligence capability. Historically, counterintelligence has been almost exclusively devoted to countering foreign services' human intelligence efforts. At the same time, other organizations like NSA have focused on protecting the U.S. information infrastructure.[27] We therefore recommend that the NCIX devote particular attention to working with agencies that already devote substantial resources to protection of the information infrastructure, looking beyond traditional "counterintelligence" agencies to NSA, other parts of the Department of Defense, the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, and the National Institute of Standards and Technology.

INSIDE THE AGENCIES

Primary responsibility for carrying out counterintelligence activities should remain with CIA, FBI, and the Department of Defense. These agencies, however, need to change the way they fulfill their missions. Under stronger NCIX leadership, they must become the core of the U.S. counterintelligence community—a community with common purpose, focus, and unity of effort.

Recommendation 3

The CIA should create a new capability dedicated to mounting offensive counterintelligence activities abroad.

The CIA should expand its current counterintelligence focus beyond the protection of its own operations to conduct a full range of counterintelligence activities outside the United States. This will require that CIA adopt the mission of protecting the equities of other U.S. government agencies overseas and exploiting opportunities for counterintelligence collection.

We recommend that CIA pursue this mission by establishing a new capability that would—along with the Agency's existing Counterintelligence Center—report to the Associate Deputy Director of Operations for Counterintelligence. This new capability would mount counterintelligence activities outside the United States aimed at recruiting foreign sources and conducting activities to deny, deceive, and exploit foreign intelligence targeting of U.S. interests. In short, the goal would be for the counterintelligence element to track foreign intelligence officers *before* they land on U.S. soil or begin targeting U.S. interests abroad. In doing so, the new capability would complement the Agency's existing defensive operations, and would provide the Intelligence Community with a complete overseas counterintelligence capability. And as with all intelligence activity, the CIA's actions—to the extent they involved U.S. persons—would continue to be subject to the Attorney General's guidelines designed to protect civil liberties.

We must stress that our recommendation is not intended to downplay the importance of continuing to protect CIA operations. These counterintelligence activities must continue, and resources currently allocated to asset validation or other operational counterintelligence capabilities should not be diminished. In this vein, we believe that case officers devoted to the new, offensive activity should be "fenced off" so that they cannot be directed to execute other tasks.

Recommendation 4

The Department of Defense's Counterintelligence Field Activity should have operational and investigative authority to coordinate and conduct counterintelligence activities throughout the Defense Department.

While our intelligence foes strategically target our defense infrastructure, the Department of Defense's counterintelligence response remains hardwired to the 1947 framework in which it was created, with each armed service running

its own counterintelligence component. In 2002, the Defense Department began to address this deficiency by creating the Counterintelligence Field Activity (CIFA), which has the authority to oversee Department of Defense "implementation support to the NCIX," complete counterintelligence program evaluations, conduct operational analysis, provide threat assessments, conduct counterintelligence training, and "oversee Defense-wide CI investigations."[28]

There is, however, one very significant hole in CIFA's authority: it cannot actually carry out counterintelligence investigations and operations on behalf of the Department of Defense.[29] Rather, Defense-wide investigations and operations are left to the responsibility of the individual services—which are, at the same time, also responsible for investigations and operations *within* their own services.[30] Perhaps unsurprisingly, the result of this arrangement is that intra-service investigations are given priority by the services, and no entity views non-service-specific and department-wide investigations as its primary responsibility. What this means is that many Defense Department components (*e.g.*, Combatant Commands, the Defense Agencies, and the Office of the Secretary of Defense) lack effective counterintelligence protection.

We believe this serious shortcoming would be best addressed by giving CIFA the authority and responsibility to provide Department-wide counterintelligence functional support by conducting investigations, operations, collection, and analysis for the Combatant Commands, Defense Agencies, and the Office of the Secretary of Defense, both inside and outside of the United States. The counterintelligence elements within each military service would be left in place to focus on their department's counterintelligence requirements. CIFA would acquire new counterespionage and law enforcement authorities to investigate national security matters and crimes including treason, espionage, foreign intelligence service or terrorist-directed sabotage, economic espionage, and violations of the National Information Infrastructure Protection Act. Specific authorization from the Secretary of Defense and a directive from the DNI can implement this change. And, as with the CIA and service elements, all of CIFA's activities that relate to U.S. persons should be performed in accordance with Attorney General-approved guidelines.

Giving CIFA additional operational authorities will make it a stronger organization better able to execute its current management responsibilities. Today the armed services are not constituted to perform the full range of counterin-

telligence functions that the Department of Defense requires. CIFA will gain greater visibility across the Department and relieve the service counterintelligence components from a responsibility that dilutes resources and effort away from their primary mission—to protect their services from foreign intelligence activities.

Recommendation 5

The FBI should create a National Security Service that includes the Bureau's Counterintelligence Division, Counterterrorism Division, and the Directorate of Intelligence. A single Executive Assistant Director would lead the Service subject to the coordination and budget authorities of the DNI.

With respect to the FBI, we are convinced that a number of significant changes need to take place, largely as part of our recommended creation of a new National Security Service within the Bureau. We address this proposal in detail in Chapter Ten (Intelligence at Home). For current purposes, we merely identify the key reasons why this reform is especially necessary in the counterintelligence field. In our view, bringing the FBI's national security elements under a single Executive Assistant Director responsible to the DNI, and therefore also to the NCIX, would improve the overall effectiveness and strategic direction of FBI counterintelligence and effectively empower analysts to direct collections, investigations, and operations.

CONCLUSION

Since the passage of the National Security Act of 1947, counterintelligence has been treated as a kind of second-class citizen in the intelligence profession. The result is that the subject is pushed to the periphery, our adversaries take advantage of our neglect, and American national security suffers. It is all too easy to forget counterintelligence because, other than periodic spy controversies, there is little public sign that we are doing it poorly. But we are. And our adversaries know it. Our recommended changes—centralizing management and planning, expanding our overseas efforts, and integrating and directing the counterintelligence components of the CIA, Department of Defense, and FBI—are long overdue and will help to stanch the hemorrhaging of our secrets and take the fight to our adversaries.

ENDNOTES

[1] A double agent is a person pretending to work as a spy for one government while actually working as a spy for another government.

[2] Christopher Andrew, *The Sword and Shield: The Mitrokhin Archive* (1999) at pp. 215-220.

[3] Richard Helms, *A Look Over My Shoulder* (2003) at pp. 34-35.

[4] Interview with National Counterintelligence Executive (March 10, 2005).

[5] Interview with National Counterintelligence Executive (Sept. 13, 2004).

[6] FBI, Title classified (Nov. 2004) at pp. 17-18.

[7] Classified intelligence report.

[8] Interview with Office of the National Counterintelligence Executive staff (March 9, 2005).

[9] In our classified report, we include statistics on the estimated Russian and Chinese intelligence presence that we cannot include in our unclassified report.

[10] *Final Report of the National Commission on Terrorist Attacks Upon the United States* (hereinafter "9/11 Commission Report") (2004) at p. 158 & nn. 54, 56; pp. 244-245 (noting al-Qa'ida's casing activities).

[11] Interview with Terrorist Threat Integration Center official (Oct. 6, 2004).

[12] Senate Committee on Homeland Security and Governmental Affairs, *The China Connection: Summary of the Committee's Findings Relating to Efforts of the People's Republic of China to Influence United States Policies and Elections* (1997) at pp. 5-9.

[13] Congress acknowledged this in 2002 when it created the NCIX and, disappointingly, not much has changed. S. Rep. No. 106-279 (2002) at p. 16 (noting inadequate coordination, cooperation, and information-sharing among agencies; a lack of strategic threat analysis; the lack of a national plan to integrate information and analysis; an inadequately prepared workforce with insufficient, diffused resources; and the lack of a national advocate and program for resources, policies, and proactive initiatives).

[14] Executive Order No. 12333 at § 1.14(a).

[15] Interview with FBI Assistant Director for Counterintelligence (Oct. 7, 2005).

[16] Executive Order No. 12333 at § 1.5(e).

[17] Interview with CIA counterintelligence official (Nov. 19, 2004).

[18] *See, e.g.*, Interview with senior official from the Office of the National Counterintelligence Executive (March 9, 2005).

[19] Interview with Department of Defense Counterintelligence and Security official (Oct. 14, 2004); Interview with Department of Defense Counterintelligence Field Activity official (Dec. 14, 2004). "The primary problem is that [Department of Defense] counterintelligence is assigned, under Title X of U.S. law, to the military services as their responsibility, controlled and conducted by them. The military services limit their counterintelligence routinely to support their own missions." Walter Jajko, "The State of Defense Counterintelligence," *Journal of U.S. Intelligence Studies* (Winter/Spring, 2004) at pp. 7-9.

[20] Department of Defense Directive No. 5105.67 (Feb. 19, 2002) at § 6.2.

[21] 50 U.S.C. at § 402b.

[22] Intelligence Authorization Act for Fiscal Year 2003 at §§ 902, 904.

[23] Intelligence Reform and Terrorism Prevention Act of 2004 at § 1011, Pub. L. No. 108-458.

[24] The concept of a Mission Manager is defined more fully in Chapter Six (Leadership and Management), Chapter Seven (Collection), and Chapter Eight (Analysis).

[25] The other exception is the director of the National Counterterrorism Center, the DNI's Mission Manager for Terrorism, who will also be responsible for producing strategic analysis.

[26] We examined other options for improving counterintelligence, but decided that a strengthened NCIX was the best and least disruptive option. Creating a separate national counterintelligence agency, for instance, would involve new legislation, a significant outlay of organizational effort and funding, and disruption of current operations.

[27] *See generally* National Intelligence Council, *Cyber Threats to the United States Infrastructure* (NIE 2004-01D/I) (Feb. 2004).

[28] Department of Defense Directive No. 5105.67 (Feb. 19, 2002) at §§ 6.2.4.1 & 6.2.9.

[29] *Id. at* § 6.2.

[30] Within the Department of Defense, counterintelligence functional support includes investigations, operations, collection, analysis, and functional services. Currently, only the Army, Navy, Air Force, and Marine Corps have authority to do all five activities.

CHAPTER TWELVE
COVERT ACTION

Most U.S. presidents have made use of covert action as an instrument of foreign policy; under appropriate and limited circumstances, it serves as a more subtle and surgical tool than acknowledged employment of U.S. power and influence. In the future, when the threats of proliferation and terrorism loom large, covert action may play an increasingly important role. The Commission conducted a careful study of U.S. covert action capabilities, with attention to the changing national security landscape and the special category of missions that involve both CIA and U.S. Special Operations Forces. Because even the most general statements about the Intelligence Community's capabilities in this area are classified, the Commission's assessments and four specific findings cannot be discussed in this report. The Commission has, however, incorporated the lessons learned from its study of covert action in all of our recommendations for reform of the Intelligence Community.

CHAPTER THIRTEEN
THE CHANGING PROLIFERATION THREAT AND THE INTELLIGENCE RESPONSE

Summary & Recommendations

The threat of chemical, biological, and nuclear weapons proliferation has transformed over the past two decades. The technical expertise required to produce these weapons has become increasingly widespread, while many of the materials needed to make them are widely available on the open market. Meanwhile, terrorists have expressed a growing demand for these weapons and demonstrated their willingness to use them. The Intelligence Community has not kept pace with these events.

Rather than attempt a top-to-bottom assessment of the chemical, biological, and nuclear weapons threat, here we focus on relatively new aspects of the threat that present specific intelligence challenges, and that—in our view—require additional Intelligence Community reforms beyond those discussed in our other chapters.

We recommend that:

- The DNI take several specific measures aimed at better collaboration between the intelligence and biological science communities;
- The National Counter Proliferation Center develop and ensure the implementation of a comprehensive biological weapons targeting strategy. This entails gaining real-time access to non-traditional information sources; filtering open source data; and devising specific collection initiatives directed at the resulting targets;
- The Intelligence Community, along with other relevant government bodies, support a more effective framework to interdict shipments of chemical, biological, and nuclear proliferation concern; and
- The Intelligence Community better leverage existing legal and regulatory mechanisms to improve collection and analysis on chemical, biological, and nuclear threats.

INTRODUCTION

We live in a world where the most deadly materials created by man are more widely available than ever before. Over the past decade or so, the proliferation of nuclear, biological, and chemical materials, and the expertise to weaponize them, has become a global growth industry.

Grim evidence of this abounds. For instance, the Soviet Union may have been relegated to the dustbin of history, but its nuclear materials—under uncertain control, and sought by rogue states and terrorists alike—still imperil our present. At the same time, terrorists who have already demonstrated their intent to attack us with anthrax seek more advanced biological and nuclear weapons. Perhaps worst of all, the biotechnology revolution is rapidly making new, previously unimagined horrors possible, raising the specter of a modern-day plague, spawned from a back room or garage anywhere in the world.

There is no single strategy the Intelligence Community can pursue to counter the "proliferation" menace. As we discuss in this chapter, any weapon capable of causing mass casualties presents a unique set of challenges. Our study of this subject indicates, however, that there are themes common to all. First, the Intelligence Community's efforts with regard to the spread of nuclear, biological, and chemical weapons have not kept up with the pace of proliferation, and urgently require improvement. We believe that catching up will likely require prioritizing counterproliferation over many other competing national security issues. It will also require more aggressive and innovative collection techniques, and the devotion of resources commensurate to the seriousness of the threat and the difficulty of the collection challenge.

Second, the Intelligence Community must reach outside its own confines to tap counterproliferation information, authorities, and expertise resident in the government and nation at large. The Community cannot expect to thwart proliferators on its own; counterproliferation is a team sport, and our squad must draw on the rest of the U.S. government and the full weight of its regulatory and diplomatic powers, as well as on scientific and technical experts from academia and private enterprise.

We begin our discussion of the proliferation problem by examining these themes within the context of the threat posed by biological weapons. Of all the potentially catastrophic threats facing the United States, those related to

biological substances are changing the most quickly, metastasizing in recent years to include a variety of new potential users and substances. Unlike nuclear or chemical weapons, a biological weapon has actually been used to attack the United States, in the form of the anthrax attacks of 2001. In our view, biological weapons are also the mass casualty threat the Intelligence Community is least prepared to face. We therefore have focused on developing recommendations that can immediately improve our capabilities in this area—by bringing into the Community much-needed scientific experience, sharpening collection techniques, and harnessing regulatory authorities to bolster intelligence efforts.

We then survey the threat landscape with regard to nuclear and chemical weapons, and follow this with a series of recommendations designed to improve overall Intelligence Community support to the interdiction of materials of proliferation concern. We close with recommendations that recognize the importance of more generally leveraging legal and regulatory mechanisms to aid in the service of intelligence.

The stakes for the Intelligence Community with regard to all weapons of mass destruction are self-evidently high. It is not hyperbole to suggest that the lives of millions, and the very fabric and fate of our society, may depend on the way in which the Community is configured, and the powers it can bring to bear against the challenges posed by proliferation. Our recommendations do not purport to solve the proliferation problem; no commission can claim to do that. We do hope, however, that the recommendations can help better configure the Community to cope with an increasingly fluid and volatile threat environment.

BIOLOGICAL WEAPONS

Introduction: "The Greatest Intelligence Challenge"

For many years, the U.S. intelligence and policy communities did not take the biological weapons threat as seriously as the dangers posed by nuclear weapons. Many felt that states might experiment with biological weapons, but would not use them against the United States for fear of nuclear retaliation. Similarly, terrorists who promised to bring "plagues" upon the United States were thought to be merely indulging in grandiose threats; they lacked the technical expertise to actually develop and deploy a biological weapon.

These views changed suddenly in September and October of 2001 when anthrax attacks in the United States killed five people, crippled mail delivery in several cities for over a year,[1] and required decontamination efforts costing more than $1 billion.[2] The still-unsolved attack was striking in its asymmetry: the anthrax could have been produced for less than $2,500.[3]

Even more striking is how lucky we were. A determined terrorist group could do far worse with only a little more effort and a bit of luck. Even allowing for imperfect dissemination techniques, if a gram of the same anthrax used in the 2001 attacks had been disseminated outdoors in an urban area, between 100 and 1,000 people would likely have been infected, and many would have died.[4] A kilogram might infect tens of thousands of people.[5] And because biological weapons have a delayed effect, terrorists could execute multiple or campaign-style attacks before the first attack is even noticed and the warning sounded.[6]

We are concerned that terrorist groups may be developing biological weapons and may be willing to use them. Even more worrisome, in the near future, the biotechnology revolution will make even more potent and sophisticated weapons available to small or relatively unsophisticated groups.

In response to this mounting threat, the Intelligence Community's performance has been disappointing. Its analyses of state and non-state biological weapons programs often rest on assumptions unsupported by data. This is in large part because traditional collection methods do not work well, or at all, against biological threats. Even though scientists, academics, and government officials routinely describe an attack with biological weapons as one of the most terrifying and probable disasters the United States faces, the Intelligence Community is lagging behind in looking for new collection strategies, and has not sought sufficient help outside the halls of intelligence agencies. The Community cannot defeat what one senior policymaker told us was "the greatest intelligence challenge" by itself.[7]

We recommend three ways of changing the Intelligence Community's overall approach to biological weapons: (1) better coordination with the biological sciences community; (2) more aggressive, targeted approaches to intelligence collection; and (3) effective use of new regulatory mechanisms to create collection opportunities.

Biological Threats*

Terrorism

Despite the possibility that terrorists have gained access to biological weapons, a large bioterrorist attack has not yet occurred. Why not? First, executing a large-scale biological attack is still fairly difficult as a technical matter; it requires organization and long-term planning. Second, biological agents can be highly infectious; working with them is dangerous. Finally, the war on terrorism may have derailed nascent attack plans. But these thin lines of defense are rapidly eroding. Some terrorist groups may have the financial resources to purchase scientific expertise. Even without sophisticated expertise, a crude delivery system would be sufficient to inflict mass disruption and economic damage.[8] Moreover, extremists willing to die in a suicide bombing are not likely to be deterred by the dangers of working with biological weapons. As a result, a senior intelligence official told the Commission that we should consider ourselves "lucky" we have not yet suffered a major biological attack.[9] And the terrorist threat will only grow, as biological weapons are rapidly becoming cheaper, easier to produce, and more effective.

States

States pose another biological weapons threat, and the weapons they produce are potentially more sophisticated—and therefore more lethal—than those made by terrorists. We can only speculate as to why countries have not yet used biological weapons on a large scale. In part, there is the risk of blowback—infection could spread to the state's own population. The United States may also be protected by the threat that it will respond violently to a biological attack. As President Nixon said when he terminated the United States biological weapons program and embraced an international ban, "We'll never use the damn germs, so what good is biological warfare as a deterrent? If somebody uses germs on us, we'll nuke 'em."[10]

Covert use, however, is an entirely different matter. If the United States is attacked with biological weapons and cannot identify the attacker, the threat of nuclear retaliation will be of little use. States might attack the United States or its military installations overseas and avoid retaliation by posing as terrorists. If the spread of illness is the first sign that such an attack has taken

* The classified version of this section contains a more detailed discussion of the nature of the biological weapons threat, and also provides examples that could not be included in an unclassified report.

place, the U.S. government may have difficulty responding effectively. In many attack simulations, U.S. biodefense capabilities struggle to simultaneously administer medical countermeasures, quarantine infected individuals, and decontaminate large areas.[11]

Biotechnology

A third biological weapons threat lies not far in the future. Terrorists may soon be able to cause mass casualties that are now possible only for state-run biological weapons programs. Scientists can already engineer biological weapons agents to enhance their lethality either through genetic engineering or other manipulations.[12] Such weapons of science fiction may soon become a fact. Given the exponential growth in this field and access to its insights through the Internet, our vulnerability to the threat might be closer at hand than we suspect.

The Intelligence Gap: What We Don't Know

The Intelligence Community has struggled to understand the biological weapons threat. According to a senior official in CIA's Counterproliferation Division, "We don't know more about the biological weapons threat than we did five years ago, and five years from now we will know even less."[13]

Analysis: Assumptions Abound

Assessments of state and non-state programs rely heavily on assumptions about potential biological weapons agents, biological weapons-adaptable delivery systems, and fragmentary threat reporting. Unsurprisingly, this leads to faulty assessments. For example, in October 2002, the Intelligence Community estimated with "high confidence" that Iraq had an active biological weapons program.[14] Yet the Iraq Survey Group's post-war investigation "found no direct evidence that Iraq had plans for a new biological weapons program or was conducting biological weapons-specific work for military purposes" after 1996.[15] In Afghanistan, the story is the reverse. Despite suspicions that al-Qa'ida had biological weapons intentions, the Intelligence Community was unaware of the ambitious scope of its efforts.[16]

Biological weapons analysis also suffers from the litany of problems we have identified elsewhere in our report, including insufficient outreach to technical experts in the CIA's Directorate of Science and Technology and the Department of Energy's National Labs, as well as those in the business community,

public heath sector, and academia.[17] With limited interaction between technical experts and political analysts, the Intelligence Community "does a poor job of matching capabilities with intent" to develop realistic biological attack scenarios for state and non-state actors alike.[18] As one National Intelligence Officer told us, biological weapons analysts have an "institutional bias against creative war-gaming" and rarely engage in systematic testing of alternative hypotheses.[19]

*Collection: Continued Frustration and a Glimmer of Hope***

The weaknesses of analysis, however, pale beside the Intelligence Community's inability to collect against the biological weapons target. We found that the Community's biological weapons collection woes result from both the technological limits of traditional collection methods and a poorly focused collection process that is ill-equipped to gather and sort through the wealth of information that could help alert the Community to crucial indicators of biological weapons activity. In our classified report, we discuss these intelligence collection limitations at length; unfortunately, these details cannot be included in our unclassified report.

At bottom, the gap in collection on the biological threat is largely attributable to the fact that the Community is simply not well configured to monitor the large stream of information—much of it publicly available—relevant to biological weapons. In our classified report, we illustrate how considerable information about al-Qa'ida's pre-war biological weapons program in Afghanistan could have been known through public or government sources; we cannot, however, provide these details in an unclassified format. We emphasize here simply that the Community must focus on doing a better job of collecting and connecting similar indicators of biological weapons personnel and activity in the future. Moreover, as we point out in our Chapter Eight (Analysis), it is essential that the Community improves its access to and use of open source intelligence—the challenges posed by the biological weapons threat reinforce that conclusion.

However, before the Community can begin to effectively monitor such vital indicators of biological activity, it must develop a basic understanding of the threat landscape. We were disappointed to discover that, three-and-a-half

**A considerable majority of information contained in this section of our classified report could not be discussed in an unclassified format.

years following the anthrax attacks, the Intelligence Community has still not taken many of the most rudimentary steps necessary for this sort of collection. In our classified report, we offer examples of how particular intelligence agencies have failed to take these steps, but these details cannot be discussed in an unclassified format. We also describe a (classified) nascent effort at CIA that we believe to be worthy of praise. In all events, the Intelligence Community must ensure that any new efforts support a comprehensive collection effort across different regions, groups, and biological threats. Just as in other areas of intelligence, agencies at times jealously guard their most sought-after information. This fragmentation and parochialism highlights the importance of integrating the government's efforts against proliferators as well as the need for naming a deputy to the Proliferation Mission Manager, as recommended below, to focus exclusively on biological weapons issues.

The United States Response: The Biodefense Shield

Although resources have flowed freely into biodefense since the 2001 anthrax attacks, only a fraction of these resources has gone to funding new intelligence collection strategies.[20] A senior official at the National Security Council laments that, with regard to biological weapons intelligence, "there's still a sense that it's too hard to do."[21] Although future biodefense technologies and medical countermeasures may allow the United States to neutralize the effects of biological attack, intelligence is one of the few tools today that holds out hope of avoiding attack, rather than just limiting the damage. Biodefense is critical, but it should not be our first line of defense. As a senior Centers for Disease Control and Prevention (CDC) official states, we "need to move upstream from the event"—a reactive biological weapons posture will not suffice.[22]

One positive outgrowth of U.S. biodefense programs is that they have bred new intelligence customers, beyond the traditional military and foreign policy users. Technical experts, who include the CDC, Department of Homeland Security, the United States Army Medical Research Institute for Infectious Diseases (USAMRIID), the National Institute for Allergies and Infectious Diseases (part of the National Institutes of Health, or NIH), and the Department of Agriculture, now need biological weapons threat information to inform their biodefense efforts.[23] The existence of these customers presents an opportunity to encourage more focused biological weapons intelligence, and in turn to provide the Intelligence Community with much needed expertise.

Regrettably, new biodefense customers are largely unaware of what intelligence can bring to the table. A senior NIH official, for example, expressed frustration with the quality of biological weapons intelligence that NIH receives, as well as the lack of a structured venue for receiving and assessing such information. This has made the effort to set vaccine research and development priorities more difficult and, worse yet, may have divorced vaccine research from what is known about the current threat.[24] Yet at the same time, demonstrating the cultural gap that still divides the biodefense and intelligence communities, this same official expressed immediate reluctance when told that NIH could perform its own intelligence analysis of open sources to identify the most likely biological threats.[25]

CIA analysts observe that their agency in particular does a poor job of interacting with outside experts,[26] but there are promising initiatives elsewhere within the Community. One effort aimed at increasing such interaction is the Defense Intelligence Agency's Bio-Chem 2020, a small-scale attempt at discussing emerging biotechnology threats with outside experts, usually at the unclassified or secret level. These scientists publish periodic papers on general biological threats rather than reviewing specific biological weapons analysis.[27] A senior National Security Council official praises Bio-Chem 2020 but is quick to note that it is a "cottage program," not part of a broader Intelligence Community endeavor.[28] Another useful initiative is a plan for a National Interagency Biodefense Campus at Fort Detrick, Maryland, with personnel from USAMRIID, NIH, and the Departments of Agriculture and Homeland Security. The campus, which is designed to coordinate biodefense research and serve as a central repository for expertise, will not be complete until 2008.[29] In our view, the culture gap between the biological science and defense communities is so large that housing them together is essential to fostering a common strategy. The extent of Intelligence Community participation at the campus, however, remains undetermined.[30]

Going Forward: Improving Biological Weapons Intelligence Capabilities

If the Intelligence Community does not improve its foreign and domestic collection capabilities for biological weapons, the risk of catastrophe will only grow. We see a need for three broad changes: (1) tighter Intelligence Community coordination with the biological science community both inside government and out; (2) far more emphasis on integrated and aggressive intelligence

targeting; and (3) stronger regulatory efforts to control potential biological weapons technologies, which would enable more intelligence collection than any go-it-alone effort by the Intelligence Community.

Working with the Biological Science Community

Recommendation 1

The DNI should create a Community-wide National Biodefense Initiative to include a Biological Science Advisory Group, a government service program for biologists and health professionals, a post-doctoral fellowship program in biodefense and intelligence, and a scholarship program for graduate students in biological weapons-relevant fields.

When an intelligence analyst wants to understand a foreign nuclear weapons program, the analyst can draw on the expertise of thousands of Americans, all of whom understand how to run a nuclear program—because that is what they do, day in and day out. If an analyst wants the same insight into biological weapons programs, working bio-weaponeers are simply not available. The last offensive American biological weapons program ended 35 years ago.

The United States faced a similar dilemma in the late 1950s with regard to nuclear physics. The World War II physicists at Los Alamos were aging, and the younger generation did not have strong ties to the U.S. government. In response, the Defense Department founded the JASONs, an elite group of distinguished nuclear scientists that interacts with senior policymakers, receives intelligence briefings, and provides classified studies on pressing national security issues.[31] Considering the number of Nobel laureates in the group, the opportunity for rising stars to interact with leading scientists in their field, and the financial compensation that members receive, membership to the JASONs remains highly coveted.

According to a CIA report summarizing a conference of life science experts, "a qualitatively different relationship between the government and life sciences communities might be needed to most effectively grapple with the future biological weapons threat."[32] Although DIA's Bio-Chem 2020 is a successful interaction mechanism with academia and the private sector, it is insufficient compared to what is required. The Intelligence Community needs more consistent advice than that provided by unpaid professionals, and more

contemporary advice than that provided by intelligence scientists who have not published research in over a decade.

We therefore recommend that the new DNI create a National Biodefense Initiative composed of several programs aimed at strengthening the Intelligence Community's biological weapons expertise. Such an initiative could be composed of the following four components:

- An elite Biological Sciences Advisory Group, administered by the DNI's Director of Science and Technology, which would be composed of the nation's leading life science experts. The group would be compensated for their work and asked to examine and advise the DNI on biological threats;
- A part-time government service program for select biologists and health professionals to review biological weapons analysis and answer Community queries;
- A post-doctoral fellowship program that funds scientists for one to two years of unclassified research relevant to biodefense and biological weapons intelligence; and
- A scholarship program that rewards graduate students in the biological weapons-relevant hard sciences in exchange for intelligence service upon completion of their degrees.

Recommendation 2

The DNI should use the Joint Intelligence Community Council to form a Biological Weapons Working Group. This Working Group would serve as the principal coordination venue for the Intelligence Community and biodefense agencies, including the Department of Homeland Security's National Biodefense and Countermeasures Center, NIH, CDC, the Department of Agriculture, and USAMRIID.

In addition to reaching *outside* the government to develop a more robust and mutually beneficial relationship with the biological science community, the Intelligence Community needs more effective links with biological experts and authorities inside the government. Nurturing this relationship will help

ensure that relevant science is informing actual intelligence collection and better serving new customers. We believe that the DNI could utilize the Joint Intelligence Community Council, established by the intelligence reform legislation, to convene a working group of agencies with interest in biological weapons intelligence to serve as a kind of "consumer council."[33] This working group would have the added benefit of helping both sides—the intelligence and biological science communities—understand the needs of the other so that they can more effectively work in parallel. The DNI might consider moving the biological weapons working group, or other biological weapons intelligence units, to the National Interagency Biodefense Campus once it is completed in 2008.

Targeting Biological Weapons Threats

Recommendation 3

The DNI should create a deputy within the National Counter Proliferation Center who is specifically responsible for biological weapons; this deputy would be responsible to the Proliferation Mission Manager to ensure the implementation of a comprehensive biological weapons targeting strategy and direct new collection initiatives.

As our previous discussion of the Community's collection woes starkly illustrates, the Intelligence Community needs more aggressive, targeted approaches to intelligence collection on biological threats. Systematic targeting of potential biological weapons personnel and programs is critical. CIA's Directorate of Science and Technology is funding some promising efforts, but they remain in their initial stages, and the Directorate lacks the authority to implement a program across the Community. Much more needs to be done.

First, the Intelligence Community needs a targeted, managed, and directed strategy for biological weapons intelligence. We strongly suggest designating an office within the NCPC to handle biological weapons specifically. It is also essential that this designee (or deputy) for biological weapons work in tandem with his or her counterparts at the National Counterterrorism Center.

With visibility across the Intelligence Community, the biological weapons deputy in the National Counter Proliferation Center (NCPC) could draw on different pockets of relevant expertise. But if CIA's Directorate of Operations

(DO) is any kind of microcosm of the biological weapons intelligence world, then a daunting task lies ahead. Within the DO, the Counterterrorist Center collects against bioterrorism; the Counterproliferation Division collects against most state biological weapons programs, and the geographic area divisions collect against the remainder.[34] Such fragmentation leaves serious potential gaps.[35]

Devising and implementing a biological weapons targeting strategy will require not only that the Intelligence Community begin to think as a whole, but also that the Intelligence Community think beyond itself. Part of the challenge involves drawing on personnel and databases housed in non-Intelligence Community agencies such as Commerce's Bureau of Industry and Security and Homeland Security's Customs and Border Protection. Data from non-intelligence sources needs to be cross-referenced with the Intelligence Community's biological weapons databases, and filtered through a set of developed biological weapons indicators to direct intelligence collection. FBI and Homeland Security personnel need training in intelligence targeting and access to this system to identify homeland threats.

A comprehensive and strategic approach to biological weapons targeting will also involve open source exploitation to drive collection and warning strategies, and a multi-year research and development plan for the development and deployment of emerging collection technologies. In our classified report, we offer several suggestions for improving the Intelligence Community's capabilities which cannot be discussed in an unclassified format. Elements within the Community deserve praise for having taken steps to implement these suggestions.

It is our hope that through a Target Development Board, the NCPC's deputy for biological weapons can drive the Intelligence Community to pursue the necessary multifaceted collection approach. We encourage the Community to continue to explore and develop new approaches to collection, and we expect that these efforts would be dramatically furthered by the Mission Manager and Target Development Board devices.

Leveraging Regulation for Biological Weapons Intelligence

Recommendation 4

The National Security Council should form a Joint Interagency Task Force to develop a counter-biological weapons plan within 90 days that draws upon all elements of national power, including law enforcement and the regulatory capabilities of the Departments of Homeland Security, Health and Human Services, Commerce, and State.

The United States should look outside of intelligence channels for enforcement mechanisms that can provide new avenues of international cooperation and resulting opportunities for intelligence collection. The National Counter Proliferation Center will be able to do a great deal to expand outreach to the biological science, biodefense, and public health sectors, but an even broader effort is required to draw on departments and agencies outside of the Intelligence Community. We believe the National Security Council or perhaps the Homeland Security Council is the most appropriate venue for convening different national security elements to devise such national-level strategies. Intelligence will be able to most effectively operate in a national security environment that is organized around and cognizant of its combined efforts to work against the biothreat.

We suggest that the Joint Interagency Task Force consider, as part of its development of a counter-biological weapons plan, the following two recommendations—which involve developing beneficial relationships with foreign states and applying regulatory powers to foreign entities that do business with the United States.

Recommendation 5

The State Department should aggressively support foreign criminalization of biological weapons development and the establishment of biosafety and biosecurity regulations under the framework of the United Nations Security Council Resolution 1540. U.S. law enforcement and intelligence agencies should jointly sponsor biological weapons information sharing events with foreign police forces.

Developing close relationships with foreign governments on the biological weapons issue will be imperative if the United States is to better achieve its goals of monitoring and containing biological threats. Perhaps most importantly, the United States can bring its powers of suasion to bear on states to adopt domestic legislation that criminalizes biological weapons and establishes domestic controls to prevent proliferation—as they are obligated to do under the terms of United Nations Security Council Resolution 1540.

Criminalization will facilitate cooperation from liaison services, which are more likely to assist the United States in contexts where their domestic laws are violated. U.S. law enforcement and intelligence agencies should make cooperation with foreign officials a priority, and should establish regular information sharing events with foreign police forces to assist them in honing their awareness of the biological weapons threat and encouraging cooperation.

Recommendation 6

The United States should remain actively engaged in designing and implementing both international and regulatory inspection regimes. It should consider extending its existing biosecurity and biosafety regulations to foreign institutions with commercial ties to the United States, using the possibility of increased liability, reduced patent protection, or more burdensome and costly inspections to encourage compliance with appropriate safeguards.

International inspections will—at least with respect to state programs—remain an important counterproliferation tool in the future.[36] Arguably, designing effective inspection regimes will become all the more critical in a future where proliferation increasingly involves countries with small (and therefore difficult to detect) chemical, biological, and nuclear weapons programs. The benefits to having on-the-ground access to suspect facilities could be substantial.

There is little prospect in the near future for an international biological weapons inspection regime, however. The United States should therefore seek to obtain some of the benefits of inspections through the use of creative regulatory approaches. One such approach would involve a traditional regulatory model of imposing obligations on international businesses. The approach would build on Executive Order 12938 as amended,[37] which directs the Sec-

retary of Treasury to prohibit the importation into the United States of products produced by a foreign person or company who "materially contributed or attempted to contribute to" the development, production, stockpiling, or acquisition of weapons of mass destruction.[38] More vigorous enforcement of this order would begin to reduce the biological weapons proliferation vulnerabilities that arise through lax internal controls in the private sector.

How might such a regime work? All companies that handle dangerous pathogens could be required to meet security standards and provide data about their facilities, as is already being done inside the United States. This need not be a unilateral undertaking. Objections from major trading partners could be reduced through cooperative inspection agreements with, for example, the United States, the European Union, and Japan. Compliance by individual companies could be ensured with a mix of carrot and stick—such as "fast lane" border controls, whereby companies that adhere to United States standards are granted speedier customs processing at our ports and airports; with the possibility of reduced liability protections and patent protections for the uncooperative.

Conclusion

Improvements in intelligence are no guarantee against a successful biological attack, but they could make such an attack substantially less likely to succeed. There are no perfect solutions, but there are better solutions than the ones we have today. For now, better is all we can do. Given the potential costs of a biological weapons attack, better is what we must do.

NUCLEAR WEAPONS

Introduction

For the Cold War-era Intelligence Community, the challenge of nuclear proliferation was menacing but manageable. The Community focused primarily on intelligence collection against a few states seeking to join the "Nuclear Club"—with an especially watchful eye directed toward states aligned with the Soviet Union.

Although tracking proliferation developments was an important and large-scale enterprise, the world's accumulated storehouse of nuclear material and

knowledge was relatively well accounted for (at least internally) by nuclear states. Moreover, the number of potential nuclear proliferators and their prospective state clients were relatively few, and the potential pathways for transferring nuclear material were reasonably well known and could be monitored—in theory at least—by traditional collection platforms.

Today's nuclear proliferation threat is much more diverse, and the challenges are more difficult. The state-based threat remains, and has been joined by the nightmarish possibility that non-state actors like terrorist groups could obtain a nuclear weapon or a "dirty bomb" and detonate it in the heart of a major American city.[39] Simultaneously, the sources of nuclear materials and expertise have themselves dramatically proliferated. The breakup of the Soviet Union has left a large body of poorly secured, dubiously inventoried nuclear materials and weapons, about which the Community knows precious little. Meanwhile, shadowy, non-state proliferation networks have appeared, quietly peddling their products to the highest bidder. These new nuclear proliferators and their customers operate under a veil of secrecy, including the use of front companies to mask their intentions and movements. It is the misfortune of our age to witness the globalization of trade in the ultimate weapon of mass destruction.

There are many facets to the nuclear proliferation problem; here we focus on but two of the most important—the availability of unsecured nuclear weapons and materials, or "loose nukes," and the appearance of non-state nuclear "brokers." We believe that the Intelligence Community must do much more to improve its collection capabilities with regard to both, for the purpose of halting nuclear proliferation at the *source*. That said, we recognize the inherent difficulty of both targets, as well as the limitations on our ability to contribute much in the way of concrete operational recommendations as to how the community can improve in this regard (other than the understandable, but rather unhelpful, advice, to "try harder" and "spend more" on the endeavor). Consequently, as we discuss later in this chapter, our recommendations focus on improving the process for interdicting nuclear materials once they are in transit from the proliferators or, as a last resort, on their way to the United States.

Loose Nukes: The Great Unknown

The single greatest hurdle to a terrorist's fabrication of a nuclear device is the acquisition of weapons-usable nuclear material.[40] If terrorists are able to pro-

cure such material intact, they can skip this most difficult part of the nuclear weapons development cycle. Just as Willie Sutton robbed banks "because that's where the money is," terrorist groups are most likely seeking nuclear material from the former Soviet Union because that is where the most material is available.[41] (Additional information concerning terrorist efforts to obtain nuclear material is presented in the classified report but cannot be discussed here.) Tracking this nuclear material in the former Soviet Union is exceedingly difficult. However, we would like to emphasize that the United States has not made collection on loose nukes a high priority.

In our classified report we discuss in greater detail the reasons why our efforts to collect intelligence in this area have struggled, and we offer suggestions for improvement that cannot be discussed in an unclassified format. While we have generally shied away from simply recommending "more" effort or funding, we believe that some of these techniques may require additional funding.

The loose nukes problem is in many ways indicative of problems facing the Intelligence Community as a whole. Analysts and collectors are too consumed with daily intelligence requirements to formulate or implement new approaches. The war on terrorism and ongoing military operations have distracted the Community from longer-term threats of critical importance to national security. The perception is that there is no "crisis" until a weapon or fissile material is stolen. The problem, of course, is that we might not know this was the case until we are jolted by news of a catastrophe in Washington, D.C. or midtown Manhattan.

Established Nuclear Powers: China & Russia

While the discussion in this section has focused on the emerging intelligence challenges resulting from the proliferation of nuclear weapons and related materials, we recognize that the traditional threat of nuclear weapons in the hands of determined state adversaries remains alive and well and requires the continued attention of policymakers and the Intelligence Community. The nuclear arsenals and emerging capabilities of China and Russia, in particular, pose a challenge to the United States—a challenge about which the Intelligence Community today knows too little. In our classified report we detail some of the struggles the Intelligence Community has had in developing information about these more traditional targets—but we cannot elaborate upon our findings in this area in this report.

The Khan Network: "One-Stop Shopping" for Proliferation

Private proliferators and the "grey market" for nuclear trafficking pose another emerging threat. States no longer have a monopoly on sophisticated nuclear technology, materials, and expertise. The insecurity of nuclear materials, combined with diffusion of the technical knowledge necessary to construct or assemble a nuclear device, has resulted in a burgeoning industry for entrepreneurial middlemen. As demonstrated in our Libya case study, this threat requires new intelligence approaches.

Former Director of Central Intelligence George Tenet has spoken publicly about the "emerging threat" posed by private proliferators like A.Q. Khan.[42] As the father of Pakistan's atomic bomb, Khan helped pioneer the practice of clandestine nuclear procurement. Through front companies, subsidiaries, and a network that stretched from Pakistan to Europe,[43] Khan sought to provide countries with "one-stop shopping" for nuclear goods. We now know that Khan's network supplied nuclear equipment and expertise that "shav[ed] years off the nuclear weapons development timelines of several states including Libya."[44] Among other things, Khan's network supplied Libya with nuclear centrifuge technology.[45]

Working alongside British counterparts, CIA's Directorate of Operations was able to penetrate and unravel many of Khan's activities through human spies. They deserve great credit for this impressive success. However, the effort dedicated to bringing down the network demonstrates how rare and hard-fought future successes may be. It is possible, although unlikely, that Khan is unique. Private dealers, after all, control many of the materials needed for nuclear weapons production.

The A.Q. Khan achievement also suggests that the Intelligence Community will meet with limited success if it acts alone. Combating proliferation networks requires insight into the networks' modes of operation; for example, understanding the front companies through which they operate. As we discuss more fully in the interdiction section below, the Intelligence Community must reach out to non-traditional partners elsewhere in the government to augment its own capabilities.

Conclusion

There is little more frightening than the thought of terrorists detonating a nuclear device within the United States. And events of the past decade—including the questionable security of former-Soviet nuclear material, the emergence of private proliferation threats like A.Q. Khan, and the rise of terrorist groups determined to strike U.S. territory—have added to the threat. Furthermore, there is no good reason to expect that North Korea and Iran will be the last states to try to acquire nuclear weapons. Indeed, acquisition by these two countries might set off a cascade of efforts by others in East Asia and the Middle East. (Nor is there a good reason to expect that states of concern will only be the neighbors of these two countries and others possessing nuclear weapons. It is worth remembering that South Africa, remote in many ways from the central regions of the Cold War, made them.) We believe that our recommendations for reform discussed elsewhere in the report, in combination with this chapter's discussion of intelligence support to interdiction and leveraging regulatory mechanisms for intelligence, will at least help the Intelligence Community be as prepared as it can be.

CHEMICAL WEAPONS

Even when unintentionally released, poisonous chemicals can have terrible effects. An accidental release of poisonous gas from a chemical plant in Bhopal, India, killed thousands in 1984.[46] Deliberate chemical attacks, of course, have the potential to be even worse. In 1995, the Japanese cult Aum Shinrikyo released the chemical nerve agent sarin on the Tokyo subway, killing twelve people, sending more than 5,500 to the hospital, and sowing fear throughout the city.[47] Commentators attributed the relatively low number of fatalities to the poor quality of the agent and Aum Shinrikyo's inefficient dispersal devices.[48] In our classified report, we offer further examples of suspected chemical weapons plots that cannot be discussed in an unclassified format.

While biological and nuclear weapons could cause the worst damage, terrorists could kill thousands of Americans by simply sabotaging industrial chemical facilities. And, due to the large volume and easy accessibility of toxic chemicals in the United States, a chemical attack causing mass casualties may be more likely than a nuclear or biological attack in the near term.

As with biological and nuclear threats, the Intelligence Community is poorly positioned to meet the challenges posed by chemical weapons. Historically, it has focused on state programs and has only recently turned its attention to potential uses of chemical weapons by terrorist groups. The Community's task is complicated by the ubiquity of toxic chemicals—which are available for sale across the United States and the world—and the relative ease with which other, even more deadly substances can be manufactured from common chemical precursors. Moreover, given the increasing sophistication of the chemical industry and the various dual uses of its products, the Community will face an increasingly difficult task in differentiating legitimate from potentially hostile manufacturing efforts. Finally, as is the case with biological weapons, many small-scale chemical production facilities can be concealed in nondescript facilities that are not easily detectable through conventional collection means, such as imagery.

The Intelligence Community certainly needs to do everything possible to collect on the plans and intentions of those terrorist groups that would use chemical weapons in an attack on the United States. Moreover, because of the easy accessibility of toxic chemicals and chemical precursors, it is essential that the Community develop strong links with the FBI, which may be better suited to monitor and respond to suspicious purchases of chemicals on the state and local level and to interface with local law enforcement for the same purpose.

Such traditional intelligence activities are necessary. But as our discussion about nuclear proliferation above demonstrates, traditional methods of intelligence collection have not proved particularly adept at monitoring "loose nukes," and there are serious questions as to whether the Community will be able to detect and disrupt new, diffuse proliferation networks that acquire and traffic in nuclear materials. Without admitting defeat, we must acknowledge the possibility that nuclear materials and perhaps nuclear weapons will find their way into the international transportation stream; bound for terrorists or rogue states, who will in turn attempt to bring them to the United States. A similarly disturbing state of affairs exists with regard to chemical weapons—as the sheer volume and availability of chemicals at home and abroad indicate that it is likely such weapons or materials will come into the hands of those who would do us harm.

As a result, it seems clear that in addition to improving its traditional collection capabilities, the Intelligence Community should also focus on improving

its capabilities with regard to directly supporting interdiction activities, both inside and out of the United States, and to fully utilizing the regulatory and legal mechanisms at our disposal for controlling proliferators. It is to these tasks that we now turn.

THE INTERDICTION CHALLENGE: INTELLIGENCE FOR ACTION

Introduction

The United States has articulated a broad and aggressive policy that emphasizes the seizure or disruption of proliferation-related materials bound for states or individuals.[49] However, the Intelligence Community is currently ill-equipped to support this policy. As one senior national security official told the Commission, counterproliferation interdiction requires "a whole intelligence support mechanism…that we don't have."[50]

First, the Intelligence Community must collect information from a wide variety of non-traditional sources, ranging from customs officials to private parties. Second, the Community must provide information to a wide variety of non-traditional customers, ranging from foreign partners to law enforcement. But perhaps most importantly, the intelligence process—collection, analysis, and dissemination—must be much faster and more action-oriented than has traditionally been the case. If intelligence officials detect information about an illicit nuclear shipment, they cannot wait weeks for their analytical units to produce "finished intelligence," or for policy entities to approve an interdiction response. In this regard, support to interdiction must resemble counterterrorism or counternarcotics intelligence support; it must be quick, integrated, and accurate.

In this section we will address the broad theme of intelligence support to the interdiction of weapons of mass destruction, and make recommendations designed to address these basic requirements. We propose a new model for coordinating and executing interdiction, as well as several specific suggestions that could improve the Community's collection efforts and help to protect our borders.

Although the discussion below could apply to any weapon of mass destruction, in the near-term it is likely to pertain primarily to nuclear devices and

chemical materials; detection and interdiction of biological substances is particularly difficult given the dual-use nature of biological equipment and the lack of discernible signatures attributed to biological materials. As was demonstrated in 2001, a biological weapon can be effectively delivered, undetected, in an envelope.

Improving the Flow of Information

To support interdiction, the Community must tap into a wide variety of information networks that are, in many cases, outside of the Intelligence Community. Counterterrorism and counternarcotics intelligence have already taken significant steps in this regard. Counterproliferation intelligence must follow suit.

One critical information source is the Department of Homeland Security, which controls several databases that can help tip off analysts and operators looking for proliferation targets. For example, two main components of Homeland Security—Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)—operate a variety of databases that follow flows of people and goods across U.S. borders. These databases provide a rich source of data for relationship mapping and link-analysis among foreign companies and individuals. Yet our interviews with operators have revealed serious information sharing problems between Homeland Security and the Intelligence Community that dramatically limit their usefulness. Our classified report offers examples of these information sharing difficulties and of one successful program run by the Office of Naval Intelligence.

Developing Tools to Do It in Real Time

Effective interdiction also requires that policymakers and operators have new analytical tools that can extract information from the Intelligence Community in real time.[51] Ships carrying nuclear material will not wait for a lengthy analysis to run its course before delivering their cargoes.

For example, to support counternarcotics interdictions Joint Interagency Task Force-South has link-analysis tools that, if shared on a government-wide basis, would permit operators to quickly establish connections among terrorist organizations, proliferation networks, and other dubious international activities.[52] Rather than starting with such existing assets, nearly every intelligence, law enforcement, or military entity involved in counterproliferation is also

developing similar tools. A National Security Council-commissioned report by the Community's Collection Concepts Development Center concluded in November 2003 that these efforts composed a "'Balkan gaggle' of sometimes redundant programs with little coordination and incomplete operational integration."[53] The DNI should use his authority to encourage development of these tools and coordinate agency efforts.

Carrying out effective interdictions also requires real time awareness of activities in the sea and the air.[54] The Coast Guard's Maritime Domain Awareness program and the recent National Security Presidential Directive articulating a Maritime Security Policy are steps in the right direction.[55] There is also an urgent need to share at least some portion of our air and maritime domain awareness information, and our computer-based tools, with international partners who will assist the United States in carrying out interdictions.

The scope of these activities demonstrates that successful interdiction requires a vision that stretches far beyond the Intelligence Community. To restate one of the primary themes we found in our study of proliferation: the Intelligence Community cannot win this battle on its own. Coordination and integration will be necessary.[56]

Going Forward: A Different Model

Currently, interdiction efforts are not sufficiently coordinated across agencies. This is particularly true with respect to operational planning and execution. We do not believe that the National Security Council is the proper locale for managing daily operations—counterproliferation or otherwise. Although the National Security Council plays a critical role in helping to develop government-wide counterproliferation policy, it should not become the center for interagency operations as the United States ramps up its interdiction capability.

Recommendation 7

The President should establish a Counterproliferation Joint Interagency Task Force to conduct counterproliferation interdiction operations; to detect, monitor, and handoff suspected proliferation targets; and to coordinate interagency and partner nations' counterproliferation activities.

A new Joint Interagency Task Force for counterproliferation would fill the role of planning and executing interdiction operations, drawing on the full range of military, law enforcement, and intelligence capabilities of the United States. Ideally, a Counterproliferation Joint Interagency Task Force would be flexible enough to support the operational needs of U.S. Strategic Command[57] or any other entity tasked with stopping, seizing, or destroying a given cargo.[58] The Task Force would contain diplomatic, military, intelligence, law enforcement, and other representatives from across the government. We recommend that it:

- Plan and execute the full range of overt and clandestine interdiction operations;
- Seek approval from the National Security Council for interdiction operational plans through the real-time decisionmaking process described below;
- Provide tactical and operational intelligence, air, and sea support to the Department of Defense Unified Commands to carry out particular operations;
- Establish the legal basis for all interdiction operations, including through agreements with consenting private sector actors and partner nations that have signed ship-boarding agreements;
- Coordinate country team and partner nation initiatives in order to defeat the flow of materials of proliferation concern; and
- Conduct regular interdiction gaming exercises with international partners to develop new operational plans and concepts.

Recommendation 8

The DNI should designate the National Counter Proliferation Center as the Intelligence Community's leader for interdiction-related issues and direct the Center to support the all-source intelligence needs of the Counterproliferation Joint Interagency Task Force, the National Security Council, and other customers.

As described in Chapter Six (Leadership and Management), our proposed National Counter Proliferation Center (NCPC) will serve a variety of functions. With regard to interdiction, the NCPC will fulfill the requirements of the Counterproliferation Joint Interagency Task Force, the National Security Council, and a growing body of counterproliferation intelligence users. Through a Target Development Board, the NCPC would prioritize and target for interdiction those proliferation networks of greatest strategic concern. Finally, the NCPC would ensure that the Intelligence Community provides the Task Force and the National Security Council with real-time proliferation intelligence support.

Recommendation 9

The President should establish, probably through a National Security Presidential Directive, a real-time, interagency decisionmaking process for counterproliferation interdiction operations, borrowing from Presidential Directive 27, the interagency decisionmaking process that supports counternarcotics interdictions.

The National Security Council currently holds a weekly interdiction sub-Policy Coordinating Committee meeting to identify potential interdiction targets and determine courses of action.[59] Since counterproliferation interdiction targets may often involve sensitive diplomatic and legal issues, the National Security Council will want to approve operational interdiction plans prior to execution. The time sensitivity of certain interdiction operations suggests that the National Security Council should adopt a virtual decision-making process-—one in which parties can consult remotely-—to accomplish this oversight function.

To streamline and clarify the counterproliferation interdiction process, we recommend a set of procedures similar to those established by Presidential Directive 27 for dealing with counternarcotics interdictions and other "types of non-military incidents."[60] Because interdictions may involve military operations that would conflict with covert activities, we recommend a separate National Security Presidential Directive that outlines the National Security Council process for supervising the planning and execution of interdiction operations. To make these decisions, National Security Council staff and senior policymakers will need intelligence to answer a range of questions.

Unlike the existing intelligence paradigm, which is heavily reliant on the production of "finished" intelligence products, interdiction may require, for example, that military commanders or customs officials communicate directly with collectors and analysts.

Recommendation 10

The State Department should enter into additional bilateral ship-boarding agreements that also help to meet the tagging, tracking, and locating requirements of the Intelligence Community and its users.

The State Department is currently charged with responsibility to secure bilateral ship-boarding agreements in support of the Proliferation Security Initiative.[61] To date, the Department has secured three important agreements.[62] We do not believe, however, that sufficient strategic thought has been directed toward how these agreements can be structured to serve intelligence purposes.

Through such bilateral agreements or related customs regulations, the State Department could, for example, require ships and aircraft to declare their locations through GPS and satellite uplink. Failure to report location information could be viewed as the rough equivalent of driving with a broken taillight, and might establish reasonable suspicion to conduct an interdiction. Such agreements and the imposition of other tracking requirements would enable intelligence to draw on new sources of data to monitor potential cargoes, vessels, and aircraft of proliferation concern.[63]

Protecting our Borders: The Department of Homeland Security

Recommendation 11

The DNI should ensure that Customs and Border Protection has the most up-to-date terrorism and proliferation intelligence. In turn, Customs and Border Protection should ensure that the National Counterterrorism Center and National Counter Proliferation Center have real-time access to its databases.

It may not be possible in all cases to identify and halt biological, nuclear, or chemical weapons shipments before they reach the United States. In such

cases, our last line of defense is detecting and stopping these shipments as they cross our border. The Department of Homeland Security, through Customs and Border Protection, collects information on incoming cargo shipments that the Intelligence Community must learn to exploit. The flip side of this equation is equally important—Customs and Border Protection needs threat information from the Intelligence Community to target shipments of concern headed to the United States. Plainly, Homeland Security and the Intelligence Community need to strengthen their relationship. A discussion of ways in which this relationship can be improved is in the classified version of our report, but cannot be discussed in an unclassified format.

If we are to increase our chances of detecting proliferation materials before they enter the United States, it is critical that Homeland Security work closely with the Intelligence Community in developing its plans for screening materials coming into the United States. Moreover, once the plans are instituted, Homeland Security and the Intelligence Community must maintain a close relationship to ensure that homeland security policies reflect the Intelligence Community's most current assessments.

Recommendation 12

The DNI and Secretary of Homeland Security should undertake a research and development program to develop better sensors capable of detecting nuclear-related materials. The effort should be part of a larger border defense initiative to foster greater intelligence support to law enforcement at our nation's borders.

The Intelligence Community's collaboration with the Department of Homeland Security should not stop at targeting cargoes. A comprehensive border defense initiative would employ an array of advanced technologies to protect our borders. For example, reconnaissance satellites, unmanned aerial vehicles, nuclear detection technologies, and biometric identification cards could all play a role in border protection.

Many critical technologies to protect the border, are still in their infancy. A senior official at the Department of Homeland Security laments that the sensors deployed at our borders are "way below ideal."[64] Customs and Border Protection officials complain that some detectors are imprecise and prone to

false alarms.[65] A concerted research and development effort is necessary to bring these technologies to maturity. A new sense of urgency is required.

ENLISTING COMMERCE AND TREASURY TO COMBAT PROLIFERATION

Introduction

The Intelligence Community will be most effective at combating chemical, biological, and nuclear threats if it works in concert with non-traditional government partners. Legal and regulatory regimes can help enable better intelligence gathering and disrupt proliferation-related activity.

On several occasions throughout our inquiry, departments and agencies outside of the Intelligence Community asked why our Commission was interested in their work. These comments illustrate the lack of connection between the Intelligence Community and large parts of the government. The Community often sees itself as a world apart, and it is viewed by outsiders as an unapproachable exotic.

In the area of proliferation in particular, such a failure to see beyond the Intelligence Community's borders—and a failure to acknowledge what intelligence can and cannot do—has deprived the country of anti-proliferation levers that it badly needs. As we saw with biological weapons, the lack of an effective (and truly reciprocal) relationship between intelligence and biological sciences has limited the Community's efforts. Similarly, the Community has not sufficiently harnessed the power of legal and regulatory regimes, and the synergies that could result from working more closely with them. While we did not seek to reach beyond the scope of our mandate, which is to study the Intelligence Community, the Commission did look at some ways in which legal and regulatory regimes might enhance intelligence collection specific to the counterproliferation issue.

We do not pretend to have weighed fully every non-intelligence interest at work in many of these regimes. For that reason, many of our recommendations only suggest areas for possible action by both the affected agency and the Intelligence Community. But regardless of whether specific regimes are instituted, we believe that closer cooperation between the Intelligence Community and the Departments of Commerce and Treasury could result in many

mutually beneficial relationships and improved collection against difficult proliferation-related targets. The Intelligence Community will be most effective at combating chemical, biological, and nuclear threats if it works in concert with non-traditional government partners.

Department of Commerce: Enforcing the Export Control Regime

The Department of Commerce's Bureau of Industry and Security (BIS) administers and enforces the Export Administration Regulations, which govern the export of dual-use items. BIS's law enforcement authorities place it in a position to collect large amounts of information that could be of great use to the Intelligence Community.

In order to obtain the cooperation of export control violators, however, BIS needs stronger law enforcement powers, something it has lacked in recent years, mainly because some of BIS's law enforcement authorities lapsed when the Export Administration Act expired. BIS could also assist the Intelligence Community more fully if it had authority to impose increased penalties for export violations and more authority to conduct undercover activities of potential intelligence value. The Administration has supported a renewal of the act that would confer these authorities, and congressional action on renewal would make cooperation between BIS and the Intelligence Community more productive.

The Export Administration Regulations provide additional opportunities to support counterproliferation efforts. Specifically, BIS inspections, the conditions BIS imposes on export licenses, and BIS's possible access to corporate records may provide valuable intelligence and counterproliferation opportunities. We discuss these and other related matters, including two classified recommendations, more fully in our classified report.

Recommendations 13 & 14

These recommendations are classified.

Department of the Treasury: Stopping Proliferation Financiers

The Treasury Department can also provide more support to counterproliferation than it does today. The Department currently has two powerful authorities with respect to terrorism that do not now apply to proliferation. The first is the authority to freeze the assets of terrorists and their financiers; the second is the authority to take action against foreign financial institutions that allow their services to be used to support terrorism. We see no reason why these same authorities should not be enhanced to also combat proliferation.

Recommendation 15

The President should expand the scope of Executive Order 13224 beyond terrorism to enable the Department of the Treasury to block the assets of persons and entities who provide financial support to proliferation.

Pursuant to the International Emergency Economic Powers Act, the President authorized the Department of the Treasury to block the assets of persons who sponsor terrorism.[66] However, Treasury lacks a similar tool to block the assets of proliferators. To fill this gap, we recommend the President take steps to allow the Secretary of the Treasury to take the same action against persons "who provide financial or other material support to entities involved in the proliferation of weapons of mass destruction." In light of the virtually universal recognition that the greatest threat the United States faces is the intersection of terrorism and proliferation, we see no reason why Treasury's authority should extend to only half of this potentially catastrophic combination.

Recommendation 16

The President should seek to have Congress amend Section 311 of the USA PATRIOT Act in order to give the Department of the Treasury the authority to designate foreign business entities involved in proliferation as "primary money laundering concerns."

Currently, section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury—in consultation with other federal officers, including the Secretary of State and the Chair of the Board of Governors of the Federal Reserve System—to designate a foreign jurisdiction or financial institution a "primary

money laundering concern," and to require that U.S. financial institutions take certain measures against the designee.[67] This power can be used when the Intelligence Community determines that a foreign financial institution is involved in proliferation-related activity. And by doing so, the Department can effectively cut the foreign institution off from the U.S. banking system. This authority is limited, however to financial institutions that assist proliferation. It would be more effective if it could also be applied to *non-financial* business entities involved in proliferation.

The reason for this suggested change is simple—many aspects of proliferation involve non-financial institutions, such as pharmaceutical, petrochemical, and high-tech companies. By limiting the Treasury Department's designation authority to financial institutions, the current law effectively addresses only one part of the business-related proliferation challenge. Expanding Treasury's authority would thus allow the U.S. government to also take action against the very businesses that supply the materials that make proliferation possible.

Specifically, we believe the Secretary's authorities should extend to the designation of individual businesses involved in proliferation as "primary money laundering concerns." Once a business was so designated, U.S. financial institutions could be required by the Treasury Department to take certain steps to avoid engaging in business transactions with the designated companies. The Secretary of the Treasury might also be able to affect whether foreign financial institutions are willing to conduct business with business entities involved in proliferation. If so, the Secretary of the Treasury could help cut off proliferators from their financial lifeblood.

Conclusion

Legal and regulatory mechanisms are valuable tools the Intelligence Community should use to their full extent. But proper use of these mechanisms requires extensive interagency cooperation. This will not be an easy task. But we believe it is a worthwhile endeavor, and one that may—in the long run—prove invaluable in combating the proliferation of nuclear, biological, and chemical weapons.

ENDNOTES

[1] Center for Counterproliferation Research, *Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks* (Nov. 2002) at p. 2.

[2] Interview with FBI official (Nov. 19, 2004).

[3] Interview with Dugway Proving Ground official (Dec. 30, 2004); *Final Report of the National Commission on Terrorist Attacks Upon the United* States (authorized edition) (2004) at p. 172 (hereinafter "9/11 Commission Report").

[4] The anthrax letter mailed to Senator Patrick Leahy had 1 trillion spores per gram. Interview with FBI special agent (Nov. 19, 2004). Inhalation of 8,000 to 10,000 spores is generally regarded as lethal, but this figure derives from studies of healthy "middle-aged" primates. Thomas V. Inglesby et al., "Anthrax as a Biological Weapon, 2002: Updated Recommendations for Management," *Journal of the American Medical Association*, vol. 287 (May 1, 2002) at pp. 2236-2252. If we accept this lethality estimate, a gram perfectly disseminated under optimal weather conditions could theoretically kill 100,000 people. Optimum weather conditions and highly efficient dissemination are unlikely, however, since weather patterns and aerosolization efficiency, among numerous other factors, would significantly alter lethality figures. National Research Council, *Making the Nation Safer* (2002) at p. 81. It is a reasonable assumption, however, that liquid or powder dissemination could kill one-thousandth to one-hundredth of those people (*i.e.*, 100 to 1,000 people). Richard Danzig, *Catastrophic Bioterrorism—What Is To Be Done?* (Aug. 2003) at pp. 1-2.

[5] In this example, a kilogram would contain 1,000 trillion anthrax spores.

[6] Richard Danzig, *Catastrophic Bioterrorism—What Is To Be Done?* (Aug. 2003) at p. 2; Brad Roberts, Institute for Defense Analyses, *Defining the Challenges of Campaign-type Responses to Campaign-type Terrorism* (Jan. 2, 2004).

[7] Interview with senior administration official (Dec. 16, 2004).

[8] NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004) at p. 24.

[9] Interview with senior intelligence official (Oct. 14, 2004).

[10] Tom Mangold and Jeff Goldberg, *Plague Wars: the Terrifying Reality of Biological Warfare* (2001) at p. 61.

[11] Tara O'Toole, Michael Mair, and Thomas Inglesby, *Shining Light on 'Dark Winter'* (2002).

[12] For example, in 2002, researchers at the University of Pittsburgh identified key proteins in *variola* (smallpox) that contribute to its virulence and demonstrated how to synthesize the virulence gene via genetic modification of smallpox's less deadly cousin *vaccina*. A. M. Rosengard, Y. Liu, Z. P. Nie, and R. Jimenez, "Variola Virus Immune Evasion Design: Expression of a Highly Efficient Inhibitor of Human Complement," *Proceedings of the National Academies of Sciences of the United States of America* (Vol. 99) (June 25, 2002) at pp. 8808-8813.

[13] Interview with senior intelligence official (Dec. 6, 2004).

[14] NIC, *Iraq's Continuing Programs for Weapons of Mass Destruction* (NIE 2002-16HC) (Oct. 2002) at pp. 5, 35. The Intelligence Community also judged that Iraq maintained delivery systems for its biological weapons agents. *Id.* at p. 7.

[15] Iraq Survey Group, *Comprehensive Report of the Special Advisor to the DCI on Iraqi*

WMD, Volume III, "Biological Warfare" (Sept. 30, 2004) at p. 1.

[16] NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004) at p. 59.

[17] Interview with senior intelligence officer (Nov. 18, 2004).

[18] Interview with senior analyst, Institute for Defense Analyses (Jan. 28, 2005).

[19] Interview with senior intelligence officer (Nov. 18, 2004).

[20] The United States spent about $14.5 billion on civilian biodefense between FY 2001 and FY 2004, and there is an additional $7.6 billion requested for FY 2005. The funds have primarily gone to the Departments of Health and Human Services (HHS) and Homeland Security (DHS), and have supported numerous initiatives to develop vaccines, environmental sensors, and emergency response capabilities. Ari Schuler, "Billions for Biodefense: Federal Agency Biodefense Funding, FY2001-FY2005," *Biosecurity and Bioterrorism: Biodefense, Strategy, Practice, and Science* (Vol. 2) (2004) at p. 86. Interview with CIA senior scientist (Jan. 18, 2005); Interview with CIA DS&T official (Jan. 19, 2005).

[21] Interview with senior administration official (Jan. 5, 2005).

[22] Interview with senior CDC official (Nov. 19, 2004).

[23] Observation made by Seth Carus, National Defense University, as related in NIC, Title Classified (NIE 2004-08HC/I) (Dec. 2004), at pp. 60-61.

[24] Interview with senior NIH official (Feb. 4, 2005).

[25] *Id.*

[26] Interview with senior intelligence official (Nov. 18, 2004); CIA has one promising effort that is in its nascent stages.

[27] Interview with CIA senior scientist (Jan. 25, 2005); Interview with biosecurity expert (Feb. 4, 2005).

[28] Interview with senior National Security Council official (Jan. 5, 2005).

[29] Interview with the Department of Homeland Security's Directorate of Science and Technology official (Nov. 15, 2004).

[30] *Id.*

[31] Ron Southwick, "Elite Panel of Academics Wins Fight to Continue Advising Military," *The Chronicle of Higher Education* (June 7, 2002). Today, the JASONs include experts from other scientific specialties as well. *Id.*

[32] CIA, Title Classified (OTI SF 2003-108) (Nov. 3, 2003)

[33] The legislation designates the Joint Intelligence Community Council as responsible for advising the DNI on "establishing requirements…and monitoring and evaluating the performance of the Intelligence Community." Intelligence Reform and Terrorism Prevention Act of 2004 at § 1031, Pub. L. No. 108-458.

[34] Classified examples concerning the Intelligence Community's collection efforts are contained in our classified report, but could not be included in an unclassified discussion.

[35] Interview with CIA senior scientist (Jan. 25, 2005).

[36] *See, e.g.*, International Atomic Energy Agency, Staff Report, *UN General Assembly Backs IAEA's "Indispensable Role"* (Nov. 2, 2004) (noting the IAEA's role in conducting inspections of nuclear programs in Iraq, Iran, and North Korea).

[37] Executive Order 12938 (amended July 28, 1998).

[38]*Id.* at § 4(a).

[39]For current purposes, we define a "dirty bomb" as a radiological dispersal device that uses the force of conventional explosives, such as TNT, to scatter radioactive material.

[40] Interview with Department of Energy intelligence analysts (Jan. 10, 2005).

[41] Interview with DIA analyst (Jan. 18, 2005).

[42] George Tenet, Remarks as prepared for delivery at Georgetown University (Feb. 5, 2004). We discuss the specifics of the A.Q. Khan story in greater detail in our classified report.

[43] *Id.*

[44] *Id.*

[45] Interview with CIA DO official (Sept. 14, 2004).

[46] Satinder Bindra, Bhopal marks chemical tragedy: 20 years since gas leak killed thousands in Indian city (Dec. 3, 2004), *available at* http://edition.cnn.com/2004/WORLD/asiapcf/12/02 /india.bhopal.mark (accessed Feb. 7, 2005).

[47] CIA, Title Classified (CTC 2003-30079H) (Aug. 7, 2003) at p. 4.

[48] *Id.*; Senate Government Affairs Permanent Subcommittee on Investigations Staff Statement, *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo* (Oct. 31, 1995), *available at* www.fas.org/irp/congress/1995_rpt/aum/part05.htm (accessed Feb. 7, 2005).

[49] National Security Presidential Directive-17 (also designated Homeland Security Presidential Directive-4) presents a broad national strategy for countering chemical, biological, and nuclear weapons proliferation that emphasizes interdiction of illicit proliferation transfers. In addition, the Proliferation Security Initiative provides a framework under which the United States and its allies have created agreements to authorize the tracking and interdicting of weapons-related shipments.

[50] Interview with senior administration official (Dec. 17, 2004).

[51] Collection Concepts Development Center, Title Classified (Nov. 21, 2003) at p. 4.

[52] *Id.* at pp. ii-iii.

[53] *Id.* at p. 46.

[54] *Id.* at p. 5.

[55] In particular, the Maritime Security Policy emphasizes the importance of a "robust and coordinated intelligence effort [that] serves as the foundation for effective security efforts in the Maritime Domain." NSC, *NSPD-41/HSPD-13: Maritime Security Policy* (Dec. 21, 2004) at pp. 5-6.

[56] A short classified section concerning how best to coordinate the government's interdiction efforts is omitted from this version of the report.

[57] The Department of Defense has recently named U.S. Strategic Command the lead Unified Command for the interdiction and elimination of weapons of mass destruction. Interview with senior Department of Defense official (Jan. 13, 2005).

[58]Officials from Special Operations Command and the Office of the Secretary of Defense for Policy have faulted the Intelligence Community for not gearing collection requirements toward sufficient levels of operational specificity, and for not quickly sharing the intelligence that is collected. Covert platforms must find an appropriate means to share ("push") information quickly to users, and users must have the capability to "pull" intelligence from the infor-

mation sharing environment with appropriate permissions and standards established by the DNI. OSD/SOLIC, *Nuclear Terrorism Intelligence: A Special Operations Perspective* (briefed on Oct. 26, 2004).

[59]Interview with former administration official (Feb. 7, 2005).

[60] Presidential Directive-27 was designed to enable expeditious decisionmaking, consider views of "concerned Departments and agencies," coordinate public statements, and "keep the White House fully informed throughout." *PD-27: Procedures for Dealing with Non-Military Incidents* (Jan. 19, 1978).

[61] The Proliferation Security Initiative is a framework under which the United States and its allies have created agreements to authorize the tracking and interdicting of weapons and materials of proliferation concern.

[62] Each of the three—Liberia, Panama, and the Marshall Islands—is significant because of the large number of vessels that are flagged there.

[63] Office of Naval Intelligence analysts confirm that this would indeed be helpful. Interview with National Maritime Intelligence Center officials (Feb. 14, 2005).

[64] Interview with Department of Homeland Security official (Oct. 7, 2004).

[65] Interview with Customs and Border Protection officials (Feb. 18, 2004). Interview with Customs and Border Protection officials (Jan. 21, 2005).

[66] Executive Order 13224 at § 1(d).

[67] 50 U.S.C. § 5318A.