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.