APPENDIX A
Authorizing Executive Order

Executive Order 13328
Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Sec. 1. Establishment. There is established, within the Executive Office of the President for administrative purposes, a Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Commission).

Sec. 2. Mission. (a) The Commission is established for the purpose of advising the President in the discharge of his constitutional authority under Article II of the Constitution to conduct foreign relations, protect national security, and command the Armed Forces of the United States, in order to ensure the most effective counter-proliferation capabilities of the United States and response to the September 11, 2001, terrorist attacks and the ongoing threat of terrorist activity. The Commission shall assess whether the Intelligence Community is sufficiently authorized, organized, equipped, trained, and resourced to identify and warn in a timely manner of, and to support United States Government efforts to respond to, the development and transfer of knowledge, expertise, technologies, materials, and resources associated with the proliferation of Weapons of Mass Destruction, related means of delivery, and other related threats of the 21st Century and their employment by foreign powers (including terrorists, terrorist organizations, and private networks, or other entities or individuals). In doing so, the Commission shall examine the capabilities and challenges of the Intelligence Community to collect, process, analyze, produce, and disseminate information concerning the capabilities, intentions, and activities of such foreign powers relating to the design, development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use, or use of Weapons of Mass Destruction, related means of delivery, and other related threats of the 21st Century.

(b) With respect to that portion of its examination under paragraph 2(a) of this order that relates to Iraq, the Commission shall specifically examine the Intel-

ligence Community's intelligence prior to the initiation of Operation Iraqi Freedom and compare it with the findings of the Iraq Survey Group and other relevant agencies or organizations concerning the capabilities, intentions, and activities of Iraq relating to the design, development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use, or use of Weapons of Mass Destruction and related means of delivery.

(c) With respect to its examination under paragraph 2(a) of this order, the Commission shall:

(i) specifically evaluate the challenges of obtaining information regarding the design, development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use, or use of Weapons of Mass Destruction, related means of delivery, and other related threats of the 21st Century in closed societies; and

(ii) compare the Intelligence Community's intelligence concerning Weapons of Mass Destruction programs and other related threats of the 21st Century in Libya prior to Libya's recent decision to open its programs to international scrutiny and in Afghanistan prior to removal of the Taliban government with the current assessments of organizations examining those programs.

(d) The Commission shall submit to the President by March 31, 2005, a report of the findings of the Commission resulting from its examination and its specific recommendations for ensuring that the Intelligence Community of the United States is sufficiently authorized, organized, equipped, trained, and resourced to identify and warn in a timely manner of, and to support United States Government efforts to respond to, the development and transfer of knowledge, expertise, technologies, materials, and resources associated with the proliferation of Weapons of Mass Destruction, related means of delivery, and other related threats of the 21st Century and their employment by foreign powers (including terrorists, terrorist organizations, and private networks, or other entities or individuals). The Central Intelligence Agency and other components of the Intelligence Community shall utilize the Commission and its resulting report. Within 90 days of receiving the Commission's report, the President will consult with the Congress concerning the Commission's report and recommendations, and will propose any appropriate legislative recommendations arising out of the findings of the Commission.

Sec. 3. Membership. The Commission shall consist of up to nine members appointed by the President, two of whom the President shall designate as Co-Chairs. Members shall be citizens of the United States. It shall take two-thirds of the members of the Commission to constitute a quorum.

Sec. 4. Meetings of the Commission and Direction of Its Work. The Co-Chairs of the Commission shall convene and preside at the meetings of the Commission, determine after consultation with other members of the Commission its agenda, direct its work, and assign responsibilities within the Commission.

Sec. 5. Access to Information. (a) To carry out this order, the Commission shall have full and complete access to information relevant to its mission as described in section 2 of this order and in the possession, custody, or control of any executive department or agency to the maximum extent permitted by law and consistent with Executive Order 12958 of April 17, 1995, as amended. Heads of departments and agencies shall promptly furnish such information to the Commission upon request. The Attorney General and the Director of Central Intelligence shall ensure the expeditious processing of all appropriate security clearances necessary for the members of the Commission to fulfill their functions.

(b) Promptly upon commencing its work, the Commission shall adopt, after consultation with the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, rules and procedures of the Commission for physical, communications, computer, document, personnel, and other security in relation to the work of the Commission. The Secretary of Defense, the Attorney General, and the Director of Central Intelligence shall promptly and jointly report to the President their judgment whether the security rules and procedures adopted by the Commission are clearly consistent with the national security and protect against unauthorized disclosure of information required by law or executive order to be protected against such disclosure. The President may at any time modify the security rules or procedures of the Commission to provide the necessary protection.

Sec. 6. General Provisions. (a) In implementing this order, the Commission shall solely advise and assist the President.

(b) In performing its functions under this order, the Commission shall, subject to the authority of the President, be independent from any executive department or agency, or of any officer, employee, or agent thereof.

(c) Nothing in this order shall be construed to impair or otherwise affect the authorities of any department, agency, entity, officer, or employee of the United States under applicable law.

(d) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(e) The Director of the Office of Administration shall provide or arrange for the provision of administrative support and, with the assistance of the Director of the Office of Management and Budget, ensure funding for the Commission consistent with applicable law. The Director of the Office of Administration shall ensure that such support and funding meets the Commission's reasonable needs and that the manner of provision of support and funding is consistent with the authority of the Commission within the executive branch in the performance of its functions.

(f) Members of the Commission shall serve without compensation for their work on the Commission. Members who are not officers or employees in the executive branch, while engaged in the work of the Commission, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Government service (5 U.S.C. 5701 through 5707), consistent with the availability of funds.

(g) The Commission shall have a staff headed by an Executive Director. The Co-Chairs shall hire and employ, or obtain by assignment or detail from departments and agencies, the staff of the Commission, including the Executive Director.

(h) The term “Intelligence Community” is given the same meaning as contained in section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4)).

(i) The term "Weapons of Mass Destruction" is given the same meaning as contained in section 1403(1) of the Defense Against Weapons of Mass Destruction Act of 1996 (50 U.S.C. 2302(1)).

Sec. 7. Judicial Review. This order is intended only to improve the internal management of the executive branch, and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

Sec. 8. Termination. The Commission shall terminate within 60 days after submitting its report.

GEORGE W. BUSH

THE WHITE HOUSE,

February 6, 2004.

APPENDIX B
List of Findings and Recommendations

PART ONE: Looking Back

Chapter 1: Iraq

Iraq Findings

Overall Commission Finding: The Intelligence Community's performance in assessing Iraq's pre-war weapons of mass destruction programs was a major intelligence failure. The failure was not merely that the Intelligence Community's assessments were wrong. There were also serious shortcomings in the way these assessments were made and communicated to policymakers.

Nuclear Weapons Summary Finding: The Intelligence Community seriously misjudged the status of Iraq's alleged nuclear weapons program in the 2002 NIE and other pre-Iraq war intelligence products. This misjudgment stemmed chiefly from the Community's failure to analyze correctly Iraq's reasons for attempting to procure high-strength aluminum tubes.

1. The Intelligence Community's judgment about Iraq's nuclear program hinged chiefly on an assessment about Iraq's intended use for high-strength aluminum tubes it was seeking to procure. Most of the agencies in the Intelligence Community erroneously concluded these tubes were intended for use in centrifuges in a nuclear program rather than in conventional rockets. This error was, at the bottom, the result of poor analytical tradecraft—namely, the failure to do proper technical analysis informed by thorough knowledge of the relevant weapons technology and practices.

2. In addition to citing the aluminum tubes, the NIE's judgment that Iraq was attempting to reconstitute its nuclear weapons program also referred to additional streams of intelligence. These other streams, however, were very thin, and the limited value of that supporting intelligence was inadequately conveyed in the October 2002 NIE and in other Intelligence Community products.

3. The other indications of reconstitution—aside from the aluminum tubes—did not themselves amount to a persuasive case for a reconsti-

tuted Iraqi nuclear program. In light of the tenuousness of this other information, DOE's argument that the aluminum tubes were not for centrifuges but that Iraq was, based on these other streams of information, reconstituting its nuclear program was a flawed analytical position.

4. The Intelligence Community failed to authenticate in a timely fashion transparently forged documents purporting to show that Iraq had attempted to procure uranium from Niger.

Biological Warfare Summary Finding: The Intelligence Community seriously misjudged the status of Iraq's biological weapons program in the 2002 NIE and other pre-war intelligence products. The primary reason for this misjudgment was the Intelligence Community's heavy reliance on a human source—codenamed "Curveball"—whose information later proved to be unreliable.

1. The DIA's Defense HUMINT Service's failure even to attempt to validate Curveball's reporting was a major failure in operational tradecraft.

2. Indications of possible problems with Curveball began to emerge well before the 2002 NIE. These early indications of problems—which suggested unstable behavior more than a lack of credibility—were discounted by the analysts working the Iraq WMD account. But given these warning signs, analysts should have viewed Curveball's information with greater skepticism and should have conveyed this skepticism in the NIE. The analysts' resistance to any information that could undermine Curveball's reliability suggests that the analysts were unduly wedded to a source that supported their assumptions about Iraq's BW programs.

3. The October 2002 NIE failed to communicate adequately to policymakers both the Community's near-total reliance on Curveball for its BW judgments, and the serious problems that characterized Curveball as a source.

4. Beginning in late 2002, some operations officers within the regional division of the CIA's Directorate of Operations that was responsible for relations with the liaison service handling Curveball expressed serious concerns about Curveball's reliability to senior officials at the CIA, but these views were either (1) not thought to outweigh analytic assessments

that Curveball's information was reliable or (2) disregarded because of managers' assessments that those views were not sufficiently convincing to warrant further elevation.

5. CIA management stood by Curveball's reporting long after post-war investigators in Iraq had established that he was lying about crucial issues.

6. In addition to the problems with Curveball, the Intelligence Community—and, particularly, the Defense HUMINT Service—failed to keep reporting from a known fabricator out of finished intelligence on Iraq's BW program in 2002 and 2003.

Chemical Warfare Summary Finding: The Intelligence Community erred in its 2002 NIE assessment of Iraq's alleged chemical warfare program. The Community's substantial overestimation of Iraq's chemical warfare program was due chiefly to flaws in analysis and the paucity of quality information collected.

1. The Intelligence Community relied too heavily on ambiguous imagery indicators identified at suspect Iraqi facilities for its broad judgment about Iraq's chemical warfare program. In particular, analysts leaned too much on the judgment that the presence of "Samarra-type" trucks (and related activity) indicated that Iraq had resumed its chemical weapons program.

2. Analysts failed to understand, and collectors did not adequately communicate, the limitations of imagery collection. Specifically, analysts did not realize that the observed increase in activity at suspected Iraqi chemical facilities may have been the result of increased imagery collection rather than an increase in Iraqi activity.

3. Human intelligence collection against Iraq's chemical activities was paltry, and much has subsequently proved problematic.

4. Signals intelligence collection against Iraq's chemical activities was minimal, and much was of questionable value.

Delivery Summary Finding 1: The Intelligence Community incorrectly assessed that Iraq was developing unmanned aerial vehicles for the purpose of delivering biological weapons strikes against U.S. interests.

Delivery Summary Finding 2: The Intelligence Community correctly judged that Iraq was developing ballistic missile systems that violated United Nations strictures, but was incorrect in assessing that Iraq had preserved its Scud missile force.

1. The Intelligence Community made too much of an inferential leap, based on very little hard evidence, in judging that Iraq's unmanned aerial vehicles were being designed for use as biological warfare delivery vehicles and that they might be used against the U.S. homeland.

2. The Intelligence Community failed to communicate adequately to policymakers the weak foundations upon which its conclusions were based.

3. The Intelligence Community failed to give adequate consideration to other possible uses for Iraq's UAVs or to give due credence to countervailing evidence.

4. The Intelligence Community was generally correct in assessing that Iraq was continuing ballistic missile work that violated United Nations restrictions, but erred in many of the specifics.

Regime Decisionmaking Summary Finding: The Intelligence Community, because of a lack of analytical imagination, failed even to consider the possibility that Saddam Hussein would decide to destroy his chemical and biological weapons and to halt work on his nuclear program after the first Gulf War.

Iraq Conclusions

1. Saddam Hussein's Iraq was a hard target for human intelligence, but it will not be the last that we face. When faced with such targets in the future, the United States needs to supplement its traditional methodologies with more innovative approaches.

2. Rewarding CIA and DIA case officers based on how many assets they recruit impedes the recruitment of *quality* assets.

3. The CIA, and even more so the DIA, must do a better job of testing the veracity of crucial human sources.

4. Iraq's denial and deception efforts successfully hampered U.S. intelligence collection.

5. In the case of Iraq, collectors of intelligence absorbed the prevailing analytic consensus and tended to reject or ignore contrary information. The result was "tunnel vision" focusing on the Intelligence Community's existing assumptions.

6. Intercepted communications identified some procurement efforts, but such intelligence was of only marginal utility because most procurements were of dual-use materials.

7. Signals intelligence against Iraq was seriously hampered by technical barriers.

8. Other difficulties relating to the security and counterintelligence methods of the Iraqi regime hampered NSA collection.

9. Traditional imagery intelligence has limited utility in assessing chemical and biological weapons programs.

10. Measurements and signatures intelligence (MASINT) collection was severely hampered by problems similar to those faced by other intelligence methods. Analysts' lack of familiarity with MASINT also reduced its role in analysts' assessments of Iraq's WMD programs.

11. Recognizing that it was having problems collecting quality intelligence against Iraq, the Intelligence Community launched an effort to study ways to improve its collection performance. This process was hampered by haphazard follow-up by some agencies; in particular, NSA failed to follow-up promptly on the Intelligence Community's recommendations.

12. Analysts skewed the analytical process by requiring proof that Iraq did not have WMD.

13. Analysts did not question the hypotheses underlying their conclusions, and tended to discount evidence that cut against those hypotheses.

14. The Community made serious mistakes in its technical analysis of Iraq's unconventional weapons program. The National Ground Intelligence Center in particular displayed a disturbing lack of diligence and technical expertise.

15. Analysis of Iraqi weapons programs was also flawed by "layering," with one individual assessment forming the basis for additional, broader assessments that did not carry forward the uncertainties underlying each "layer."

16. Analysis of Iraq's weapons programs took little account of Iraq's political and social context. While such a consideration would probably not have changed the Community's judgments about Iraq's WMD, the failure even to *consider* whether Saddam Hussein had elected to abandon his banned weapons programs precluded that possibility.

17. The Community did not adequately communicate uncertainties about either its sources or its analytic judgments to policymakers.

18. The Community failed to explain adequately to consumers the fundamental assumptions and premises of its analytic judgments.

19. Relevant information known to intelligence collectors was not provided to Community analysts.

20. Relevant information known to intelligence analysts was not provided to Community collectors.

21. Inability to obtain information from foreign liaison services hampered the Community's ability to assess the credibility of crucial information.

22. The President's Daily Brief (PDB) likely conveyed a greater sense of certainty about analytic judgments than warranted.

23. The National Intelligence Estimate process is subject to flaws as well, and the Iraq NIE displays some of them. The length of the NIE encourages policymakers to rely on the less caveated Key Judgments. And the language of consensus ("most agencies believe") may obscure situations in which the dissenting agency has more expertise than the majority.

24. The Iraq NIE was produced to meet a very short deadline. The time pressure was unfortunate and perhaps avoidable, but it did not substantially affect the judgments reached in the NIE.

25. The shortened NIE coordination process did not unfairly suppress the National Ground Intelligence Center's slightly more cautious estimates of Iraq's CW stockpile.

26. The Intelligence Community did not make or change any analytic judgments in response to political pressure to reach a particular conclusion, but the pervasive conventional wisdom that Saddam retained WMD affected the analytic process.

27. The CIA took too long to admit error in Iraq, and its Weapons Intelligence, Nonproliferation, and Arms Control Center actively discouraged analysts from investigating errors.

Iraq Recommendation

The Director of National Intelligence should hold accountable the organizations that contributed to the flawed assessments of Iraq's WMD programs.

Chapter 2: Libya Findings

1. The Intelligence Community accurately assessed what nuclear-related equipment and material had been obtained by Libya, but it was less successful in judging how well Libya was able to exploit what it possessed.

2. The Intelligence Community's central judgment that Libya possessed chemical weapons agents and chemical weapons aerial bombs was correct, but Libya's actual chemical agent stockpile proved to be smaller in quantity than the Intelligence Community estimated.

3. The Intelligence Community's assessment that Libya maintained the desire for an offensive biological weapons program, and was pursuing at least a small-scale research and development effort, remains unconfirmed.

4. The Intelligence Community's assessments of Libya's missile programs appear to have been generally accurate, but it is not yet possible to evaluate them fully because of limited Libyan disclosures.

5. The Intelligence Community's penetration of the A.Q. Khan proliferation network provided invaluable intelligence on Libya's nuclear efforts.

6. The Intelligence Community's performance with regard to Libya's chemical and biological programs was more modest, due in part to the limited effectiveness of technical collection techniques against these targets.

7. The Intelligence Community gathered valuable information on Libya's missile program.

8. Analysts generally demonstrated a commendable willingness to question and reconsider their assessments in light of new information.

9. Analysts tracking proliferation program developments sometimes inappropriately equated procurement activity with technical capabilities, and many analysts did not receive the necessary training to avoid such failings.

10. Analytic products sometimes provided limited effective warning to intelligence consumers, and tended to separate WMD issues from broader discussions of political and economic forces.

11. Shifting priorities and the dominance of current intelligence production leave little time for considering important unanswered questions on Libya, or for working small problems that might prove to have an impact on reducing surprise over the long term.

Chapter 3: Al-Qa'ida in Afghanistan Findings

1. Information obtained through the war in Afghanistan and in its aftermath indicated that al-Qa'ida's biological weapons program was further along than analysts had previously assessed.

2. Analytic judgments regarding al-Qa'ida's chemical weapons capabilities did not change significantly as a result of the war.

3. The war in Afghanistan brought to light detailed and revealing information about the direction and progress of al-Qa'ida's radiological and nuclear ambitions.

4. Intelligence gaps prior to the war in Afghanistan prevented the Intelligence Community from being able to assess with much certainty the extent of al-Qa'ida's weapons of mass destruction capabilities.

5. Analysis on al-Qa'ida's potential weapons of mass destruction development in Afghanistan did not benefit from leveraging different analytic disciplines.

6. Analysts writing on al-Qa'ida's potential weapons of mass destruction efforts in Afghanistan did not adequately state the basis for or the assumptions underlying their most critical judgments. This analytic shortcoming is one that we have seen in our other studies as well, such as Iraq, and it points to the need to develop routine analytic practices for quantifying uncertainty and managing limited collection.

Chapter 4: Terrorism Findings

1. Although terrorism information sharing has improved significantly since September 11, major change is still required to institute effective information sharing across the Intelligence Community and with state, local, and tribal governments.

2. Ambiguities in the respective roles and authorities of the NCTC and CTC have not been resolved, and the two agencies continue to fight bureaucratic battles to define their place in the war on terror. The result has been unnecessary duplication of effort and the promotion of unproductive competition between the two organizations.

3. Persisting ambiguities and conflicts in the roles, missions, and authorities of counterterrorism organizations hamper effective warning.

4. Persistent ambiguities and conflicts in the roles, missions, and authorities of counterterrorism organizations with regard to analysis and warning have led to redundant efforts across the Community and inefficient use of limited resources.

5. The failure to manage counterterrorism resources from a Community perspective has limited the Intelligence Community's ability to understand and warn against terrorist use of weapons of mass destruction.

Chapter 5: Iran and North Korea

The eleven findings in this chapter are classified.

PART TWO: Looking Forward
The Recommendations

Chapter 6: Leadership and Management

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.

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."

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

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.

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

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.

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.

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

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

Chapter 7: Collection

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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 Commu-

nity-wide Inspector General in the Office of the DNI, if such an office is established.

Chapter 8: Analysis

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

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.

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.

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."

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.

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.

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.

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

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

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.

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.

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

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.

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.

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.

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.

Chapter 9: Information Sharing

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;
- 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.

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.

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;

- 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.

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.

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

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.

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.

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.

Chapter 10: Intelligence at Home

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.

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

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.

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

Chapter 11: Counterintelligence

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.

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.

3. The CIA should create a new capability dedicated to mounting offensive counterintelligence activities abroad.

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.

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.

Chapter 12: Covert Action

The four recommendations in this chapter are classified.

Chapter 13: The Changing Proliferation Threat and the Intelligence Response

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.

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.

3. The DNI should create a deputy within the National Counter Proliferation Center that 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.

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.

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.

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.

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.

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.

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.

10. The State Department should enter into additional bilateral shipboarding agreements that also help to meet the tagging, tracking, and locating requirements of the Intelligence Community and its users.

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.

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.

13. *This recommendation is classified*.

14. *This recommendation is classified*.

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.

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."

APPENDIX C
An Intelligence Community Primer

INTRODUCTION

The U.S. Intelligence Community is a federation of executive branch agencies and organizations that work—both together and separately—to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. While the U.S. Intelligence Community is a large and complex organization, its primary mission is clear-cut: to collect and convey essential information needed by the President and other members of the U.S. policymaking, law enforcement, and military communities for the performance of their duties and responsibilities. This includes collecting and assessing information concerning international terrorist and narcotic activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States. The President also may direct the Intelligence Community to undertake special activities, including covert action, as needed to support intelligence collection activities and to protect against foreign threats to U.S. security interests.

The purpose of the following discussion is to provide an overall picture of the U.S. Intelligence Community today and how it functions. It is intended as a primer for readers who may be unfamiliar with the subject.

MEMBERS OF THE U.S. INTELLIGENCE COMMUNITY

The U.S. Intelligence Community comprises 15 federal agencies, offices, and elements of organizations within the Executive branch that are responsible for the collection, analysis, and dissemination of intelligence. These include fourteen departmental components—eight in the Department of Defense, two in the Department of Homeland Security, one each in four other departments (State, Energy, Treasury, and Justice) and one independent agency, the Central Intelligence Agency. Each member of the Community provides a unique set of capabilities to bear upon the intelligence challenges facing the U.S. government. The members of the Intelligence Community are:

Independent Component

***Central Intelligence Agency (CIA)*:** CIA collects intelligence, principally through human means, and provides comprehensive, all-source analysis related to national security topics for national policymakers, defense planners, law enforcement officials, and the military services. CIA also conducts counterintelligence overseas and undertakes special activities at the direction of the President.

Department of Defense Components

***Defense Intelligence Agency (DIA)*:** DIA provides comprehensive, all-source, foreign-military intelligence for the military services, policymakers, and defense planners.

***National Security Agency (NSA)*:** NSA collects and processes foreign signals intelligence information for members of the policymaking and military communities and protects critical U.S. information systems from compromise.

***National Geospatial-Intelligence Agency (NGA)*:** NGA provides geospatial intelligence (described below) in support of national security and Department of Defense missions.

***National Reconnaissance Office (NRO)*:** NRO designs, builds, operates, and maintains the nation's reconnaissance satellites.

***Army, Navy, Air Force, and Marine Corps intelligence organizations*:** Each service collects and processes intelligence relevant to its particular needs.

Non-Defense Departmental Components

***Department of State/Bureau of Intelligence and Research (INR)*:** INR provides analysis of global developments to the State Department and contributes its unique perspectives to the community's National Intelligence Estimates.

***Department of Justice/Federal Bureau of Investigation (FBI)*:** FBI takes responsibility for intelligence issues related to counterespionage, terrorism and counterintelligence inside the United States, threats to homeland security, and data about international criminal cases. Because of its law enforcement mission, the FBI is not, in its entirety, part of the Intelligence Community.

***Department of Homeland Security/Directorate of Information Analysis and Infrastructure Protection*:** This component of DHS monitors, assesses, and coordinates indications and warnings of threats to the U.S. homeland; gathers and integrates terrorist-related information; and assesses and addresses the vulnerabilities of the nation's critical infrastructures.

***Department of Homeland Security/U.S. Coast Guard Intelligence*:** Coast Guard Intelligence assesses and provides information related to threats to U.S. economic and security interests in any maritime region including international waters and America's coasts, ports, and inland waterways.

***Department of Energy (DOE)/ Office of Intelligence (IN)*:** The Department of Energy's Office of Intelligence performs analyses of foreign nuclear weapons, nuclear nonproliferation, and energy-security related intelligence issues in support of U.S. national security policies, programs, and objectives.

***Department of Treasury/Office of Terrorism and Financial Intelligence (INF)*:** Treasury's intelligence component collects and processes information that bears on U.S. fiscal and monetary policy and threats to U.S. financial institutions.

All the responsibilities of the CIA, DIA, NSA, NRO, and NGA are related to intelligence, and therefore each of these organizations in its entirety is considered a member of the Intelligence Community. The other departments and military services listed above are concerned primarily with business and missions other than intelligence and therefore only parts of their organizations are considered part of the Intelligence Community. For example, in the case of the U.S. Navy, only the Office of Naval Intelligence (ONI) is considered a member of the Intelligence Community.

In addition to the fifteen organizations listed above, the Intelligence Community also has established a number of *national centers* such as the Counterterrorist Center (CTC); Weapons Intelligence, Nonproliferation, and Arms Control Center (WINPAC); and the Crime and Narcotics Center (CNC). There is also a national center created by statute—the National Counterterrorism Center (NCTC), created by the *Intelligence Reform and Terrorism Prevention Act of 2004*. These centers are staffed by personnel from organizations across the Intelligence Community and are responsible for

developing collaborative approaches to collection and analysis of intelligence on specific issues.

WHAT IS INTELLIGENCE?

Intelligence is knowledge about the world around us that will help our civilian and military leaders make more informed decisions and prepare for and counter potential and emerging threats to U.S. interests. Intelligence starts with information obtained in response to known or perceived requirements from senior policymakers, defense and law enforcement officials, and military commanders. While some of this information may be available to the public, much of it is concealed by those governments or organizations (such as terrorists) who wish it to remain secret. Thus, such information derives typically from human or technical sources gathered in a clandestine manner. Collecting such denied information is a key responsibility of the Intelligence Community.

There are five primary categories or "disciplines" of information that the Intelligence Community seeks to collect to satisfy the needs of senior policymakers, decisionmakers, and military officials. Sometimes also referred to as collection techniques, these disciplines are:

Human intelligence, or HUMINT, consists of information obtained from individuals who know or have access to sensitive foreign information that has implications for U.S. security interests. The CIA and the Defense HUMINT Service, an element of the Defense Intelligence Agency, and, more recently, the FBI, are the primary collectors of HUMINT for the Intelligence Community.

Signals intelligence, or SIGINT, is information derived from intercepted communications and electronic and data transmissions. NSA is the primary collector of SIGINT for the Intelligence Community.

Imagery intelligence, or IMINT, which is also referred to as geospatial intelligence or GEOINT, is the exploitation and analysis of imagery and other geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on earth. NGA has the primary responsibility for coordinating the collection and processing of IMINT data for the Intelligence Community.

Measurement and Signature Intelligence, or MASINT, describes a category of technically derived information that provides distinctive characteristics of a specific event such as a nuclear explosion, or locates, identifies, and describes distinctive characteristics of targets through such means as optical, acoustic, or seismic sensors. The intelligence organizations within the Department of the Defense—especially DIA, NGA, and the military services—are the primary collectors of MASINT.

Open source intelligence, or OSINT, refers to publicly available information appearing in print or electronic form.

Collected information is often described as *raw intelligence* until it can be sorted, integrated, and evaluated by intelligence analysts who seek to derive meaning and understanding from the information regarding its implications for U.S. interests. Often such information can only provide an incomplete picture of the threats facing the United States. Some collected information may also be contradictory and even deceptive, planted by foreign powers intent on masking their true intentions. Analysts therefore have to supplement the collected information with their own skills, experiences, and expertise to make judgments as to the validity and likely meaning of all the information available to them. Their analysis and judgments are then conveyed to policymakers, defense and law enforcement officials, and the military services in the form of *finished intelligence* reports and briefings.

THE INTELLIGENCE CYCLE

The process of tasking, collecting, processing, analyzing, and disseminating intelligence is called the *intelligence cycle*. The intelligence cycle drives the day-to-day activities of the Intelligence Community. It starts with the needs of those who are often referred to within the Intelligence Community as intelligence "consumers"—that is, policymakers, military officials, and other decisionmakers who need intelligence information in conducting their duties and responsibilities. These needs—also referred to as intelligence requirements—are sorted and prioritized within the Intelligence Community, and are used to drive the collection activities of the members of the Intelligence Community that collect intelligence. Once information has been collected it is processed, initially evaluated, and reported to both consumers and so-called "all-source" intelligence analysts at agencies like the CIA, DIA, and the State Department's Bureau of Intelligence and Research. All-source analysts are responsible for

performing a more thorough evaluation and assessment of the collected information by integrating the data obtained from a variety of collection agencies and sources—both classified and unclassified. This assessment leads to a finished intelligence report being disseminated to the consumer. The "feedback" part of the cycle assesses the degree to which the finished intelligence addresses the needs of the intelligence consumer and will determine if further collection and analysis is required. The cycle, as depicted in the figure below, is thus repeated until the intelligence requirements have been satisfied.

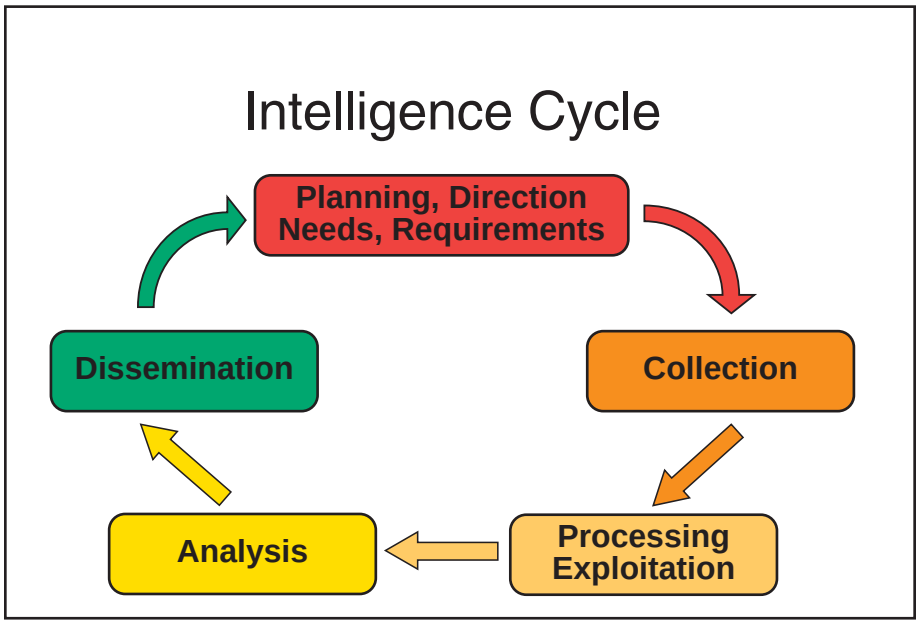

Figure 1. The Intelligence Cycle

OTHER INTELLIGENCE ACTIVITIES: COUNTERINTELLIGENCE AND COVERT ACTION

Counterintelligence encompasses actions taken to detect and counteract foreign intelligence activity that adversely affects U.S. national security interests. The FBI is the government's primary organization responsible for counterintelligence within U.S. borders, and addresses foreign intelligence services operating within the United States. CIA has the primary responsibility for conducting counterintelligence abroad. A number of other departments and agencies maintain counterintelligence elements to protect their own oper-

ations and activities within their own organizations, including the Army, Navy, and Air Force, and the Department of Energy. The Counterintelligence Field Activity (CIFA) has broad responsibilities for counterintelligence across the Department of Defense, while the National Counterintelligence Executive (NCIX) is responsible for coordinating and overseeing counterintelligence across the Intelligence Community.

Covert action is defined as activity undertaken by the U.S. government that is designed to influence foreign governments, events, organizations, or persons in support of U.S. policy and security interests in a manner that is not attributable to the United States. Typically, covert actions are carried out by CIA with such assistance as may be necessary by other elements of the Intelligence Community as directed by the President. U.S. law requires that all covert actions be approved prior to their execution by the President in a written *"finding"* and that notification be provided to the two intelligence committees in Congress. Covert actions may involve political, economic, propaganda, or paramilitary activities.

A NEW MANAGEMENT STRUCTURE FOR THE INTELLIGENCE COMMUNITY: THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

The *Intelligence Reform and Terrorism Prevention Act of 2004* established the position of the Director of National Intelligence (DNI) to serve as head of the Intelligence Community and act as the principal adviser to the President on intelligence matters related to national security. The creation of the DNI separates the responsibilities of leading the Intelligence Community from heading the CIA, which had been combined in the position of Director of Central Intelligence (DCI) previously. As we discuss in our report, the legislation gives the DNI new authorities and responsibilities that the DCI did not possess under prior law.

The DNI will be assisted in his responsibilities by the Principal Deputy Director for National Intelligence and up to four Deputy Directors for National Intelligence. The Intelligence Reform and Terrorism Prevention Act also established that the Office of the DNI (ODNI) will contain the following components to assist the DNI in his leadership of the Intelligence Community:

The National Counterterrorism Center (NCTC) serves as the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. The NCTC also conducts strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies. Other national centers that may be created in addition to NCTC (for example, a new ***National Counter Proliferation Center***) would also be part of the ODNI.

The National Intelligence Council (NIC) is responsible for producing National Intelligence Estimates (NIEs) for the U.S. government and evaluating community-wide collection and production of intelligence by the Intelligence Community.

The National Counterintelligence Executive (NCIX) is responsible for improving the performance of the counterintelligence community in assessing, prioritizing and countering intelligence threats to the United States and providing integration of counterintelligence activities of the U.S. government.

The Director for Science and Technology (DST) is to act as the chief representative of the DNI for science and technology and to assist the DNI in formulating a long-term strategy for scientific advances in the field of intelligence.

A Civil Liberties Protection Officer will ensure that the protection of civil liberties and privacy is appropriately incorporated into the policies and procedures developed by the ODNI.

A General Counsel will serve as the chief legal officer for the ODNI.

The statute also establishes the ***Joint Intelligence Community Council***, which consists of the heads of each Department that contains a component of the Intelligence Community (*e.g.*, Secretary of Defense), and which will assist the DNI in developing and implementing a joint, unified national intelligence effort to protect national security.

U.S. INTELLIGENCE RESOURCES

The intelligence resources of the United States—including manpower and funding—are grouped primarily into three categories: the National Intelligence Program, the Joint Military Intelligence Program, and Tactical Intelligence and Related Activities.

***The National Intelligence Program (NIP)*:** The *Intelligence Reform and Terrorism Prevention Act of 2004* provides the DNI with the authority to develop the budget and allocate resources under the NIP. NIP resources support national intelligence priorities and are applied to intelligence activities outside the Department of Defense and a sizable portion of the intelligence activities of the military departments and defense agencies. The agencies and organizations whose resources are included as part of the NIP include the CIA, NSA, DIA, NGA, NRO, and the intelligence elements of the Department of State, Department of Justice, Department of Energy, and Department of the Treasury.

The recent legislation provides a role for the DNI in transferring and reprogramming funds and personnel within the NIP. The Act provides the DNI with the authority to transfer funds within the NIP to an intelligence activity that is of a higher priority or in support of an emergent need, to improve program effectiveness, or increase efficiency. Such transfers or reprogramming of funds must have the approval of the Director of the Office of Management and Budget and be made in consultation with the heads of the affected department and agencies with the Intelligence Community. In addition, the transfer or preprogramming of funds for these purposes out of any agency or department funded in the NIP in a single fiscal year is not to exceed $150 million annually—or five percent of an agency or department's budget under the NIP—without approval of the head of the department or agency affected. The DNI is also authorized to transfer up to 100 people to a new intelligence center within the first twelve months of the establishment of that center, with the approval of the Director of the Office of Management and Budget and in consultation with the appropriate congressional committees. Intelligence resources under JMIP and TIARA (described below) will continue to be managed by the Department of Defense and the military services; however the DNI will participate in the development of the JMIP and TIARA budgets.

***The Joint Military Intelligence Program (JMIP)*:** The JMIP encompasses military intelligence activities that support Defense-wide objectives, as opposed to a single military service. The JMIP falls under the authority of the Secretary of Defense. JMIP resources support multiple defense organizations across functional boundaries and mission areas. Many of the programs under JMIP parallel those in the NIP. As a result, some agencies, like NGA, receive funding from both the NIP and JMIP budgets. The Deputy Secretary of Defense oversees the day-to-day activities of the Defense Department, which include the Defense Department's intelligence efforts. The Under Secretary of Defense for Intelligence serves as the JMIP Program Executive and provides policy, substantive, and programmatic guidance for the programs, projects, and activities within the JMIP.

***Tactical Intelligence and Related Activities (TIARA)*:** TIARA also falls under the authority of the Secretary of Defense and represents an aggregation of intelligence activities funded by each of the military services and the Special Operations Command to meet their specific requirements.

THE BUDGET PROCESS

Managing the annual intelligence budget can be a lengthy and complex process. As provided for in the *Intelligence Reform and Terrorism Prevention Act*, the process starts with the DNI providing guidance to the heads of agencies and organizations within the Intelligence Community for developing the NIP budget based on the priorities set by the President. The DNI will also participate in the development of JMIP and TIARA budgets managed by the Secretary of Defense including providing budget guidance to those elements of the Intelligence Community not within the NIP. This new participatory role has yet to be clearly defined. After the heads of the agencies and organizations within the Intelligence Community respond with their budget proposals and, as appropriate, after obtaining the advice of the Joint Intelligence Community Council, the DNI develops and determines the annual consolidated NIP budget. The DNI then presents the consolidated NIP budget, along with any comments from the heads of the agencies and departments containing organizations within the Intelligence Community, to the President for approval. After the NIP budget is approved and authorized, the DNI will manage the appropriations for the NIP by directing the allocation of such appropriations through the heads of the departments containing agencies or organizations within the Intelligence Community and the Director of the Cen-

tral Intelligence Agency. The DNI also will monitor the implementation and execution of the NIP by the heads of the elements of the Intelligence Community that manage programs and activities that are part of the NIP, which may include audits and evaluations.

OVERSIGHT OF THE INTELLIGENCE COMMUNITY

The Intelligence Community is subject to both Executive and Legislative oversight.

The National Security Council (NSC) is the senior Executive Branch entity that provides guidance for and direction to the conduct of national foreign intelligence and counterintelligence activities. The statutory members of the NSC are the President, the Vice President, the Secretary of State, and the Secretary of Defense.

The President's Foreign Intelligence Advisory Board (PFIAB) reviews the performance of all Government agencies involved in the collection, evaluation, or production of intelligence or in the execution of intelligence policies. The PFIAB also assesses the adequacy of management, personnel, and organization in the intelligence agencies and makes recommendations to the President for actions to improve U.S. intelligence efforts. The Intelligence Oversight Board is a standing committee of the PFIAB and is the White House entity with oversight responsibility for the legality and propriety of intelligence activities.

The Office of Management and Budget, as part of the Executive Office of the President, reviews intelligence budgets with respect to all presidential policies and priorities.

The Senate Select Committee on Intelligence (SSCI) and ***the House of Representatives Permanent Select Committee on Intelligence (HPSCI)*** are the two committees of Congress with primary jurisdiction for oversight of the Intelligence Community. These committees, along with the House and Senate Armed Services, Senate Foreign Relations, House International Relations, House and Senate Judiciary, and House and Senate Homeland Security Committees, are also charged with authorizing the programs of the intelligence agencies and overseeing their activities. The appropriation committees, by virtue of their constitutional role to appropriate funds for all U.S. Government activities, also exercise some oversight functions over the Intelligence Community.

APPENDIX D
Common Abbreviations

BIS	Bureau of Industry and Security (Department of Commerce)
BW	Biological Weapons *or* Biological Warfare
CBP	Customs and Border Protection (Department of Homeland Security)
CBRN	Chemical, Biological, Radiological and Nuclear Weapons
CCDC	Collection Concepts Development Center
CDC	Centers for Disease Control and Prevention
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity (Department of Defense)
CPD	Counterproliferation Division (CIA)
CTC	Counterterrorist Center
CW	Chemical Weapons *or* Chemical Warfare
D&D	Denial and Deception
DCI	Director of Central Intelligence
DCIA	Director of Central Intelligence Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DO	Directorate of Operations (CIA)
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DS&T	Directorate of Science and Technology (CIA)
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FIG	Field Intelligence Group (FBI)
FISA	Foreign Intelligence Surveillance Act
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency
IAEC	Iraqi Atomic Energy Commission

ICE	Immigration and Customs Enforcement (Department of Homeland Security)
INC	Iraqi National Congress
INR	Bureau of Intelligence and Research (Department of State)
INS	Immigration and Naturalization Services
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISB	Intelligence Science Board
ISE	Information Sharing Environment
ISG	Iraq Survey Group
ITIC	Intelligence Technology Innovation Center
JAEIC	Joint Atomic Energy Intelligence Committee
JICC	Joint Intelligence Community Council
JITF-CT	Counterterrorism Joint Intelligence Task Force
JMIP	Joint Military Intelligence Program
JTTF	Joint Terrorism Task Force
MASINT	Measurement and Signature Intelligence
NCIX	National Counterintelligence Executive
NCPC	National Counter Proliferation Center
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NIC	National Intelligence Council
NIE	National Intelligence Estimate
NIH	National Institutes of Health
NIO	National Intelligence Officer
NIP	National Intelligence Program
NIU	National Intelligence University
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OIPR	Office of Intelligence Policy Review (Department of Justice)
PDB	President's Daily Brief
PFIAB	President's Foreign Intelligence Advisory Board

PTTR	President's Terrorism Threat Report
SEIB	Senior Executive Intelligence Brief
SEVIS	Student and Exchange Visitor Information System
SIGINT	Signals Intelligence
SOF	Special Operations Forces
SSCI	Senate Select Committee on Intelligence
STRATCOM	U.S. Strategic Command
TDB	Target Development Board
TIARA	Tactical Intelligence and Related Activities
TTIC	Terrorist Threat Integration Center
UAV	Unmanned Aerial Vehicles
UNMOVIC	United Nations Monitoring, Verification, and Inspection Commission
UNSCOM	United Nations Special Commission
USAMRIID	U.S. Army Medical Research Institute for Infectious Diseases
UNVIE	U.S. Mission to International Organizations in Vienna
WINPAC	Weapons Intelligence, Nonproliferation and Arms Control Center (CIA)
WMD	Weapons of Mass Destruction

APPENDIX E
Biographical Information for Commissioners and List of Commission Staff

Commission Co-Chairmen

Charles S. Robb is a former Virginia Governor and U.S. Senator. As a Marine Corps officer during the 1960s, he commanded an infantry company in combat in Vietnam and, as a senator during the 1990s, he became the only member ever to serve simultaneously on all three national security committees. Robb received his law degree from the University of Virginia, clerked on the U.S. Court of Appeals for the Fourth Circuit, and practiced law with Williams and Connolly in the 1970s and Hunton and Williams in the 1980s. Since leaving public office he has been a Professor of Law and Public Policy at George Mason University, served as a Fellow at the Institute of Politics at Harvard and at the Marshall Wythe School of Law at The College of William & Mary, and Chaired the Board of Visitors at the U.S. Naval Academy.

Judge Laurence H. Silberman is a senior circuit judge on the U.S. Court of Appeals for the District of Columbia Circuit. He was a member of the U.S. Foreign Intelligence Surveillance Court of Review. The intelligence court, created in 1978, is charged with overseeing sensitive law enforcement surveillance by the U.S. government. Judge Silberman has served as Under Secretary of Labor, Deputy U.S. Attorney General, and Ambassador to Yugoslavia. From 1981 to 1985 he was a member of both the General Advisory Committee on Arms Control and the Department of Defense Policy Board. Judge Silberman was appointed to the bench by President Reagan in 1985.

Commissioners

Richard C. Levin, the Frederick William Beinecke Professor of Economics, was appointed the twenty-second President of Yale University in 1993. Before becoming president, he chaired the economics department and served as dean of the Graduate School. Dr. Levin was a member of the President's Commission on the United States Postal Service and currently is a director of the Hewlett Foundation, Lucent Technologies, Satmetix, and the National Academy of Sciences' Board on Science, Technology and Economics Policy. He also chairs the board of AllLearn, a joint venture of Yale, Oxford, and Stanford Universities.

Senator John McCain of Arizona is the senior senator from his state and has served in that chamber since 1986. He began his political career in 1982 as a U.S. Congressman from Arizona. In 2000, he sought the Republican presidential nomination. Senator McCain serves as chairman of the Commerce, Science, and Transportation Committee, and he is a member of the Armed Services and Indian Affairs committees. In January 2004, Senator McCain called for an independent inquiry into pre-war intelligence on Iraq.

Henry S. Rowen is a senior fellow at the Hoover Institution. He is also Director emeritus of the Asia/Pacific Research Center at Stanford University and Professor of Public Policy and Management emeritus at the university's Graduate School of Business. He is currently doing research on regions of innovation and entrepreneurship throughout Asia and on economic and political topics in Asia. From 1989 to 1991, Rowen was the Assistant Secretary of Defense for International Security Affairs in the U.S. Department of Defense. He was Chairman of the National Intelligence Council from 1981 to 1983, served as President of the RAND Corporation from 1968 to 1972 and was Assistant Director of the U.S. Bureau of the Budget from 1965 to 1966.

Walter B. Slocombe has held several high-level positions in the Department of Defense, including Under Secretary of Defense for Policy from 1994 to 2001; Principal Deputy Under Secretary for Policy from 1993 to 1994; Deputy Under Secretary for Policy Planning from 1979 to 1981; and Principal Deputy Assistant Secretary for International Security Affairs from 1977 to 1979. During May-November 2003 he was Senior Advisor to the Coalition Provisional Authority in Baghdad for National Security and Defense. Mr. Slocombe is currently a member of the Washington, D.C. law firm Caplin & Drysdale, chartered.

Admiral William O. Studeman (Ret.) was Deputy Director of the Central Intelligence Agency from 1992 to 1995. He has held several high-level intelligence positions, including Director of the National Security Agency and Director of Naval Intelligence. He is a former Vice President and Deputy General Manager for Intelligence and Information Superiority at Northrop Grumman Mission Systems, a $5 billion global defense contractor. He retired from the Navy in 1995 and Northrop Grumman in 2005.

Charles M. Vest served as president of MIT from 1990 to 2004. He chaired the U.S. Department of Energy Task Force on the Future of Science Programs

from 2002 to 2003. From 1993 to 1994, Dr. Vest chaired the President's Advisory Committee on the Redesign of the International Space Station, and from 1994 to the present he served as a member of the President's Council of Advisors on Science and Technology. He is a director of DuPont, IBM, and the Kavli Foundation.

Judge Patricia Wald served from 1999 to 2001 as a judge of the International Criminal Tribunal for the Former Yugoslavia at the Hague, Netherlands. An expert in international humanitarian law, she served 20 years on the U.S. Court of Appeals for the District of Columbia Circuit, including five years as chief judge. She was appointed by President Carter in 1979. Prior to her service on the bench, she served as Assistant Attorney General for Legislative Affairs from 1977 to 1979.

Lloyd Cutler *(Of Counsel)* is a founding partner of Wilmer Cutler Pickering Hale and Dorr LLP and served as counsel to Presidents Clinton and Carter. Mr. Cutler was a member and chairman of the Quadrennial Commission on Legislative, Executive, and Judicial Salaries, and a member of the President's Commission on Federal Ethics Law Reform in 1989.

Executive Director

Vice Admiral John Scott Redd (Ret.) served 36 years in the U. S. Navy, commanding eight organizations at sea from a destroyer to a fleet. He founded and commanded the Navy's Fifth Fleet in the Middle East in 1995 and served in several high-level policy positions in the Pentagon, including Director of Strategic Plans and Policy (J-5) on the Joint Staff. Since retiring in 1998 he has served as CEO of a high-tech education company and as Deputy Administrator/Chief Operating Officer of the Coalition Provisional Authority in Iraq.

General Counsel

Stewart A. Baker is a partner with the Washington, D.C. law firm of Steptoe and Johnson, LLP. He served as general counsel to the National Security Agency, deputy general counsel, Department of Education, law clerk to U.S. Supreme Court Justice John Paul Stevens, law clerk to the Honorable Frank M. Coffin, U.S. Court of Appeals, First Circuit, and the Honorable Shirley M. Hufstedler, U.S. Court of Appeals, Ninth Circuit. Mr. Baker also served on the

Markle Foundation Task Force on National Security in the Information Age, a Defense Science Board panel on Information Warfare, and the President's Export Council Subcommittee on Encryption.

Deputy Directors

Michael F. Munson *(Director for Plans)* is the former Deputy Director of the Defense Intelligence Agency. He has served as a Deputy Director for the National Reconnaissance Office and Director of Intelligence Program Review for the office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence. Mr. Munson was also the study director for the Congressionally chartered National Defense Panel. He has 35 years of intelligence experience.

Gordon C. Oehler *(Director for Review)* served for 25 years at the Central Intelligence Agency in a variety of technical and managerial positions. From April 1992 through October 1997, Dr. Oehler directed the DCI's Non-Proliferation Center and is recognized as one of the nation's leading experts on technology, proliferation, and weapons of mass destruction.

Professional Staff

John E. Antonitis
Intelligence Professional

Margaret K. Baldwin
Information Technology Specialist

Orrie B. Bayliss
Information Technology Specialist

Shaba T. Bedney
Administrative Assistant

Shelley Lea Bennett
Intelligence Professional

James B. Bruce
Intelligence Professional

B. Belinda Canton
Intelligence Professional

Thomas G. Chappell
Executive Assistant

Felix J. Ciarlo
Consultant

Elbridge A. Colby
Intelligence Professional

Sean J. Coleman
Intelligence Professional

Joan L. C. Comtois
Administrative Assistant

Jeffrey R. Cooper
Consultant

Dylan D. Cors
Intelligence Professional

Michael R. Davis
Intelligence Professional

Sean B. Davis
Intelligence Professional

Diana L. Dieckhoff
Document Control Officer

Marsha L. Dimel
Human Resources Liaison

Harvey Dixon
Information Technology Specialist

Sarah S. Erwin
Executive Assistant

Andrew M. Fialdini
Intelligence Professional

Daniel J. Flynn
Intelligence Professional

Kenneth M. Geide
Intelligence Professional

Brett C. Gerry
Deputy General Counsel & Assistant Director

Ashley Godwin
Director of Staff Operations and Finance

Irvin Gray
Director of Staff Operations and Finance

John A. Hartford, Jr.
Intelligence Professional

Kate Heinzelman
Intelligence Professional & Special Assistant to the General Counsel

Robert A. Herd
Intelligence Professional

R. Evans Hineman
Consultant

John C. Hoffman
Intelligence Professional

Joseph H. Holthaus
Security Manager

William C. Hopkins
Intelligence Professional

Penelope S. Horgan
Intelligence Professional

Darrin A. Hostetler
Associate General Counsel & Intelligence Professional

Paul M. Johnson
Intelligence Professional

Arthur Jones
Chief of Staff

Tiffany N. Kennedy
Document Control Officer

James C. King
Intelligence Professional

Armad J. Kittrell
Information Technology Specialist

Timothy R. Kochman
Information Technology Manager

Carl J. Kropf
Public Affairs Officer

Allen L. Krum
Intelligence Professional

Philip H. Kunsberg
Deputy Director for Plans

Thomas D. Lehrman
Intelligence Professional

Michael E. Leiter
Deputy General Counsel & Assistant Director

George Lemus
Information Technology Specialist

Justin B. Longcor
Facilities and Logistics Manager

Jerry D. McEntire
Intelligence Professional

Laurence J. McQuillan
Consultant

Robert P. Morean
Deputy Director for Review

Brandon J. Murray
Information Technology Specialist

Lori E. Murray
Consultant

Peter Christopher Murray
Intelligence Professional

Dennis M. Nagy
Intelligence Professional

Julia Nesheiwat
Intelligence Professional

Robert A. Pattishall
Intelligence Professional

William R. Piekney
Intelligence Professional

Lois E. Ponikvar
Executive Assistant

Glenn D. Preston
Intelligence Professional

John J. Quattrocki
Intelligence Professional

Paul J. Redmond
Intelligence Professional

Keith E. Rice
Information Technology Specialist

Doreen G. Romero
Executive Assistant

Beth N. Sauter
Document Control Officer

Abe Schachter
Information Technology Specialist

Steven T. Schanzer
Intelligence Professional

Andrew M. Shepard
Intelligence Professional

Teresa L. Smetzer
Consultant

Kelley Brooke Snyder
Associate General Counsel & Intelligence Professional

Suzanne E. Spaulding
Consultant

Michael K. Stransky
Intelligence Professional

John K. Strother
Intelligence Professional

Robert J. Surrette
Intelligence Professional

Patrick T. Toohey
Intelligence Professional

Monica D. Trachsel
Intelligence Professional

George Tsakiris
Information Technology Specialist

Marc A. Viola
Intelligence Professional

Samuel S. Visner
Consultant

Nancy M. Wheeler
Intelligence Professional

William Wilber
Security Officer

Edward M. Wittenstein
Intelligence Professional & Special Assistant to the General Counsel

Shirley Cassin Woodward
Associate General Counsel & Chief Iraq Investigator

Donald J. Wurzel
Intelligence Professional