CONFERENCE MATERIAL

DAY ONE

SPONSORED BY:

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON LAW AND NATIONAL SECURITY

CENTER FOR NATIONAL SECURITY LAW
UNIVERSITY OF VIRGINIA SCHOOL OF LAW

CENTER ON LAW, ETHICS AND NATIONAL SECURITY
DUKE UNIVERSITY SCHOOL OF LAW

CENTER ON NATIONAL SECURITY AND THE LAW
GEORGETOWN LAW

DECEMBER 1----DECEMBER 2, 2011

RITZ-CARLTON HOTEL
SALONS I AND II
1150 22ND STREET, NW
WASHINGTON, DC
## Conference Material: Day One

### Panel I
**Executive Update on Developments in National Security Law**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Order 13587 of October 7, 2011</td>
<td>1</td>
</tr>
<tr>
<td>Speech by Jeh C. Johnson to the Heritage Foundation</td>
<td>7</td>
</tr>
<tr>
<td>Statement before the House Committee on Intelligence by Robert Litt</td>
<td>17</td>
</tr>
<tr>
<td>Nomination of Robert Litt to be GC, ODNI and Stephen Preston to be GC, CIA</td>
<td>23</td>
</tr>
<tr>
<td>Committee Questions- Nominations of Robert Litt and Stephen Preston</td>
<td>45</td>
</tr>
<tr>
<td>Foreign Spies Stealing US Economic Secrets in Cyberspace</td>
<td>95</td>
</tr>
<tr>
<td>The CIA's Office of General Counsel – A. John Radwan</td>
<td>121</td>
</tr>
<tr>
<td>Statement before the Subcommittee on Crime and Terrorism by Lisa O. Monaco</td>
<td>167</td>
</tr>
<tr>
<td>The Criminal Justice System as a Counterterrorism Tool: A Fact Sheet</td>
<td>173</td>
</tr>
<tr>
<td>Attorney General Eric Holder Speaks at the American Constitution Society</td>
<td>175</td>
</tr>
<tr>
<td>Law Enforcement as a Counterterrorism Tool – David S. Kris</td>
<td>179</td>
</tr>
</tbody>
</table>

### Panel II
**Congressional Update on Developments in National Security Law**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detainee Provisions in the National Defense Authorization Bills</td>
<td>283</td>
</tr>
<tr>
<td>The New SASC Detention Bill: An Analysis of Changes and Issues – Robert Chesney</td>
<td>319</td>
</tr>
<tr>
<td>Letter to the Honorable Carl Levin</td>
<td>331</td>
</tr>
<tr>
<td>Letter to the Honorable Harry Reid</td>
<td>333</td>
</tr>
<tr>
<td>Critique of the SASC National Defense Authorization Act</td>
<td>336</td>
</tr>
<tr>
<td>Speech by Mike Rogers to American Enterprise Institute</td>
<td>339</td>
</tr>
<tr>
<td>Section 1031 of the NDAA and Other Issues It Raises – Robert Chesney</td>
<td>345</td>
</tr>
<tr>
<td>Detention Authority and Section 1031 of the NDAA – Robert Chesney</td>
<td>347</td>
</tr>
<tr>
<td>Unrest in Syria and the U.S. Sanctions Against the Asad Regime</td>
<td>349</td>
</tr>
<tr>
<td>Iran Sanctions – Kenneth Katzman</td>
<td>371</td>
</tr>
<tr>
<td>Iran’s Nuclear Program: Tehran’s Compliance with International Obligations – Paul K. Kerr</td>
<td>447</td>
</tr>
</tbody>
</table>

### Panel III
**Kosovo, Libya and Presidential War Powers for Multilateral Humanitarian Interventions**

<table>
<thead>
<tr>
<th>Title and Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testimony by Legal Advisor Harold Hongju Koh on Libya and War Powers</td>
<td>465</td>
</tr>
<tr>
<td>Authority to Use Military Force in Libya – Memorandum Opinion for the Attorney General</td>
<td>479</td>
</tr>
<tr>
<td>The War Powers Outside the Courts – William Michael Treanor</td>
<td>493</td>
</tr>
<tr>
<td>Declarations of War and Authorizations for the Use of Military Force</td>
<td>505</td>
</tr>
<tr>
<td>Memorandum on the Authorization for Use of Military Force Against Iraq</td>
<td>515</td>
</tr>
<tr>
<td>Executive Power in Wartime – Robert F. Turner</td>
<td>525</td>
</tr>
</tbody>
</table>
Panel I:

Executive Update on Developments in National Security Law

Moderator:
Harvey Rishikof
Executive Order 13587 of October 7, 2011

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and
(a) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch’s successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD–1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM–ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailers, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies
and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD-42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent’s responsibilities, in addition to those specified by NSD-42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent’s timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:
(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the Insider Threat Program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions. (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(f) of Executive Order 13526 of December 29, 2009.


(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12329, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM–ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD–42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD–42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower
Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:
(1) the authority granted by law to an agency, or the head thereof; or
(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
October 7, 2011.
Cully, thank you for that introduction, and thank you for the invitation to speak to this distinguished organization.

Someone once told me that at some point in the history of the Department of the Defense, the job of General Counsel was a relatively sleepy one. In fact, I came to the job with the belief, based on prior experience, that an agency general counsel should rarely if ever be publicly seen or heard. But when I returned to the Pentagon in February 2009, after being away for 8 years, I found a very different place.

The office of General Counsel of the Defense Department -- particularly in the post 9/11 world -- is in the middle of many difficult, front page issues: Guantanamo Bay, military commissions, operations in Libya, the legal contours of our counterterrorism efforts, Don't Ask, Don't Tell, Wikileaks, Bradley Manning, the state secrets privilege. Google search my name and you will even find a number of hits about the controversy I stirred when I sent a letter to Congress stating DoD’s opposition to a bill to rename the “Department of the Navy” the “Department of the Navy and the Marine Corps.”

On a regular basis now, when I read the newspaper in the morning, I discover a story or an op-ed with a public account of private legal advice I have supposedly offered in internal government deliberations.

Particularly as I look around this room at all the distinguished guests and journalists, I find that some people are actually interested in what the General Counsel of the Defense Department has to say.

Therefore, policy and politics aside, at every opportunity I have before civilian audiences, I devote part of my remarks to paying tribute to the sacrifices and dedication of the men and women in the U.S. military. It is the case that less than 1% of the U.S. population does the fighting for all the rest of us. These remarkable men and women in the post-9/11 military have volunteered out of a sense of public service, patriotism and selfless duty to a larger cause. Each time I read a list of those who pay the ultimate price, the most painful thing to read are the ages -- 20, 21, 22, not much older than my own teenage son. These young people gave their lives for their country before they ever really had a chance to

\[\text{As delivered, minus the personal anecdote at the beginning.}\]
know what life is all about—many will never know the joy of marriage, of parenting a son or daughter, and so many other experiences that a full life has to offer.

Then there are those who survive their injuries and must struggle on without an arm, a leg, or something else the rest of us take for granted.

Navy Lieutenant Brad Snyder is the nephew of one of my deputies. He was a member of an explosive ordnance disposal team in Afghanistan. On September 7, Lieutenant Snyder went into a mined area to clear a safe passage for a medic trying to get to others who had been wounded in action. An IED exploded in his face, severely injuring him and taking his eyesight, probably for the rest of his life. Despite his injuries and the loss of his sight, Lieutenant Snyder refused a stretcher and managed to guide the medic to those who were wounded.

One of the most remarkable things about those seriously wounded in action is the powerful sense of unit cohesion and dedication they retain even after they are injured and taken out of the fight. Within hours, they will frequently express an impatient desire to rejoin their buddies in their unit and continue service. I’ll never forget the amputee at Bethesda who asked me: “Mr. Johnson, do you think this will affect my ability to get a command?” When Lieutenant Snyder learned that the Secretary of Defense was about to visit him at Bethesda, Brad said to his mother: “I need to get out of bed and stand at attention, but I have no pants!”

For their sacrifice on behalf of the rest of us, and their dedication to our country, polls indicate that the U.S. military is the most respected and revered institution in America today.

I am convinced that one of the other reasons our military is so revered and respected is that, for all its power, we place sharp limits on the military’s ability to intrude into the civilian life and affairs of our democracy. This is a core American value that is part of our heritage, dating back to before the founding of our country.

The Declaration of Independence listed among our grievances against the King the fact that he had “kept among us, in times of peace, Standing Armies without the Consent of our legislatures,” and had “quarter[ed] large bodies of armed troops among us.” This value is reflected in the Federalist Papers, and the father of our Constitution, James Madison, wrote: “A standing military force, with an overgrown Executive, will not long be safe companions to liberty. The means of defense against foreign danger have been always the instruments of tyranny at home.”

2
This core value and this heritage is today reflected in such places as the Third Amendment, which prohibits the peacetime quartering of soldiers in private homes without consent, and in the 1878 federal criminal statute, still on the books today, which prohibits willfully using the military as a posse comitatus unless expressly authorized by Congress or the Constitution.

This brings me to the point of these remarks today:

There is danger in over-militarizing our approach to Al Qaeda and its affiliates. There is risk in permitting and expecting the U.S. military to extend its powerful reach into areas traditionally reserved for civilian law enforcement in this country. Against an unconventional non-state actor that does not play by the rules, operates in secret, observes no geographic limits, constantly morphs and metastasizes, and continues to look for opportunities to export terrorism to our Homeland, we must use every tool at our disposal. The military should not, and cannot be, the only answer.

Recent events remind us that broad assertions of military power can provoke controversy and invite challenge. Over-reaching with military power can result in litigation in which the courts intrude further and further into our affairs, and can result in national security setbacks, not gains — a point best illustrated by the question Donald Rumsfeld once asked my predecessor: “So I’m going to go down in history as the only secretary of defense to have lost a case to a terrorist?”

Particularly when we attempt to extend the reach of the military on to U.S. soil, the courts resist, consistent with our core values and our heritage.

We have worked to make military detention, in particular, less controversial, not more. The overall goal should be to build a counterterrorism framework that is legally sustainable and credible, and that preserves every lawful tool and authority at our disposal. This has meant, as the president’s counterterrorism advisor John Brennan said recently, an approach that is “pragmatic, neither a wholesale overhaul nor a wholesale retention of past practices.”

To build that less controversial, more credible and sustainable legal framework, we have in the last several years accomplished the following:

We have applied the standards of the Army Field Manual to all interrogations conducted by the federal government in the context of armed conflict.
Where appropriate, in the context of terrorist activity, we have invoked the “public safety” exception to the *Miranda* rule created by the Supreme Court in *New York v Quaries* – ensuring that the opportunity to gather valuable intelligence is fully utilized, and, at the same time, preserving the prosecution option.

We worked with the Congress to bring about a number of reforms reflected in the Military Commissions Act of 2009, and, following that, we issued a new Manual for Military Commissions. By law, use of statements obtained by cruel, inhuman and degrading treatment – what was once the most controversial aspect of military commissions – is now prohibited.

We accomplished those reforms working with a *bipartisan* coalition in Congress, and with the full support of the JAG leadership in the military.

We have appointed the highly respected former Judge Advocate General of the Navy, retired Vice Admiral Bruce Macdonald, to be the convening authority for military commissions, appointed a recognized military justice expert, Marine Colonel Jeff Caldwell, to be chief defense counsel, and this month appointed Brigadier General Mark Martins, a West Point valedictorian, Harvard Law School graduate, and Rhodes Scholar to be the chief prosecutor. We are recruiting the “A team” for this system.

We have reformed the rules for press access to military commissions proceedings, established a new public website for the commissions system, and in general, built what I believe is a credible, sustainable and more transparent system.

In the habeas litigation brought by Guantanamo detainees, lawyers in the Department of Justice and the Department of Defense have worked hard to build credibility with the courts, by conducting a thorough scrub of the evidence and the intelligence before we put forward our case for detention in the courts.

We have refined existing systems for periodic review for the cases of detainees at Guantanamo and at Bagram in Afghanistan.

Overall, the hard work of many civilian and military counterterrorism professionals, spanning both this Administration and the last, is producing results.

First and foremost, we have been aggressive and focused in the fight against Al Qaeda. Where necessary, we have not hesitated to use lawful, lethal force against Al Qaeda and its affiliates, and we are literally taking the fight to them, where they plot, where they meet, where they plan, and where they train to export terrorism to the United States. Counterterrorism experts state publicly that Al Qaeda senior leadership is today severely crippled and degraded.
Second, just as we brought justice to the man who ordered the attacks on 9/11, we seek to bring to justice KSM and the other alleged planners of 9/11, in reformed military commissions. New charges have also been referred in the case of the alleged Cole bomber, Hussayn Muhammed Al-Nashiri.

Third, the government is seeing consistent success in the habeas cases brought by Guantanamo detainees. The courts have largely recognized and accepted our legal interpretation of our detention authority, and the government has now prevailed at the District Court level in more than 10 consecutive habeas cases brought by Guantanamo detainees. We are seeing similar good results in the D.C. Circuit.

In the D.C. Circuit, the Department of Justice successfully defended against an effort to extend the habeas remedy to detainees held in Afghanistan.

Fourth, through the interrogation of those captured by the United States and our partners overseas, we continue to collect valuable intelligence about Al Qaeda, its plans and its intentions.

Fifth, this Administration, like its predecessors, continues to successfully prosecute terrorists in our federal civilian courts.

As a former federal prosecutor, I know firsthand the strength, security and effectiveness of our federal court system, and I know Cully agrees with me on this point. Given the reforms since 9/11, the federal court system is even more effective. And, as a result of lengthy and mandatory minimum prison sentences authorized by Congress and the Federal Sentencing Guidelines, those convicted of terrorism-related offenses often face decades, if not life, in prison.

The results speak for themselves. Since 9/11, numerous individuals have been convicted of terrorism-related offenses. In the last two years alone, we have seen in our federal courts a guilty plea from the man who admitted plotting to bomb the New York subway system, a guilty plea from the man who tried to bomb the commercial aircraft over Detroit on Christmas Day 2009, a life sentence imposed on the individual who attempted to detonate a bomb in Times Square, and a life sentence imposed for participation in the 1998 bombing of our embassies in Kenya and Tanzania. Going back decades, the Department of Justice has successfully prosecuted hundreds of terrorism-related cases.

Despite our successes, we know that the fight is not over. We know there is still great danger. Though degraded and on the run, we know that, in this post-Bin Laden period, Al Qaeda and its affiliates still remain determined to conduct
terrorist attacks against the United States. We know also that while Al Qaeda’s core is degraded, it is a far more decentralized organization than it was 10 years ago, and relies on affiliates to carry out its terrorist aims. We know that Al Qaeda is likely to continue to metastasize and try to recruit affiliates to its cause.

These terrorist threats are increasingly complex, multi-faceted, and defy easy labeling and categorization. Just within the last several months, we have seen terrorists who in my judgment:

- claim affiliations to more than one terrorist organization;
- belong to one terrorist organization and serve as the conduit to another;
- fit within our military detention authority but not our military commissions jurisdiction;
- fit within our military commissions jurisdiction but not the military detention authority stemming from the 2001 Authorization for the Use of Military Force; and
- fit within neither our military detention authority nor our commissions jurisdiction, but can be prosecuted in our federal civilian courts.

On top of this are Al Qaeda’s concerted efforts to recruit via the internet, with a reach in to the United States. Over and over again, we see individuals within the United States who self-radicalize and who find vindication for their hatred toward America in Al Qaeda’s ideology and propaganda. In dealing with this category of people who are here in the United States — who have never trained at an Al Qaeda camp in Afghanistan, or never sworn bayat to an Al Qaeda leader — we must guard against any impulse to label that person part of the congressionally-declared enemy, to be dealt with by military force. There is no jurisdiction to try U.S. citizens in military commissions, and our prior efforts in this conflict to put in to military detention those arrested on U.S. soil led to protracted litigation in which the government narrowly prevailed in the federal appellate courts.

As I said before, the military cannot always be the first and only answer. This is contrary to our heritage and, in the long run, will undermine our overall counterterrorism efforts.
In responding to threats and acts of terrorism, we must build a legally sustainable arsenal, and have all the legally available tools in the arsenal – whether it is lethal force against a valid military objective, military detention, interrogation, supporting the counterterrorism efforts of other nations, or prosecution in federal court or by military commissions.

Against this backdrop, we confront a series of laws and pending legislation concerning detainees, that limit the Executive Branch’s and the military’s counterterrorism options, complicate our efforts to achieve continued success, and will make military detention more controversial, not less. Here are some specific examples:

Section 1032 of the 2011 Defense Authorization Act prohibits the use of Defense Department funds to transfer any Guantanamo detainee to the United States for any conceivable purpose, no waivers or exceptions, including federal prosecution or to be a cooperating witness in a federal prosecution. Given the lengthy prison sentences mandated by Title 18 and the Sentencing Guidelines and the range of offenses available for prosecution under Title 18, there are some instances in which it is simply preferable and more effective to prosecute an individual in our federal civilian courts.

Section 1033 of the same law requires that, before the government can transfer a Guantanamo detainee to a foreign country, my client the Secretary of Defense must personally certify to the Congress certain things about the detainee and the transferee country, unless there is a court order directing the detainee’s release. After living with this provision now for almost a year, I will tell you that it is onerous and near impossible to satisfy. Not one Guantanamo detainee has been certified for transfer since this legal restriction has been imposed.

Rigid certification requirements reduce our ability to pursue the best options for national security in an evolving world situation, and intrude upon the Executive Branch’s traditional ability to conduct foreign policy – in this case, to determine when sending a detainee to another country for prosecution or reintegration would better serve our national security and foreign policy interests. Our Nation is not the only one Earth that can deal effectively with this issue. The other potential consequence of such a rigid certification requirement is that it incentivizes the Executive Branch to leave to the courts the hard work of determining who can and should remain at Guantanamo. We want the courts less involved in this business, not more.

Certain legislative proposals for the 2012 Defense Authorization Act are equally problematic.
Section 1039 of the House version of the bill prohibits the use of Department of Defense funds to transfer to the United States any non-U.S. citizen the military captures anywhere in the world as part of the conflict against Al Qaeda and its affiliates -- no waivers and exceptions. Within the national security community of the Executive Branch, we have determined that such an unqualified, across-the-board ban is not in the best interests of national security. Suppose the military captures a dangerous terrorist, and doubts arise about our detention authority overseas? Suppose the military captures an individual who, it turns out, would be vital as a cooperating witness in a terrorist prosecution in the United States? Must the option to take bring these individuals to a civilian courtroom in the U.S. be prohibited by law?

Likewise, Section 1046 of the House bill imposes an across-the-board requirement that, if military commissions jurisdiction exists to prosecute an individual, we must use commissions, not the federal courts, for the prosecution of a broad range of terrorist acts. Decisions about the most appropriate forum in which to prosecute a terrorist should be left, case-by-case, to prosecutors and national security professionals. The considerations that go into those decisions include the offenses available in both systems for prosecuting a particular course of conduct, the weight and nature of the evidence, and the likely prison sentence that would result if there is a conviction. A flat legislative ban on the use of one system -- whether it is commissions or the civilian courts -- in favor of the other is not the answer.

Section 1036 of the House bill rewrites the periodic review process the President’s national security team carefully crafted for Guantanamo detainees designated for continued law of war detention. The proposed congressional rewrite mandates the use of “military review panels,” contrary to our best judgment. Our experience shows that interagency review is valuable and preferred, to take advantage of the expertise and perspectives across the national security community in our government.

Finally, Section 1032 of the Senate version of the 2012 Defense Authorization bill includes what has come to be known as the “mandatory military custody” provision. Basically, it requires that certain members of Al Qaeda or its affiliates “be held in military custody pending disposition under the law of war,” unless the Secretary of Defense, in writing, agrees to give them up.

For starters, the trigger for this requirement is unclear. Some of my friends on the Hill say that the provision is intended to apply only to those who have been “captured in the course of hostilities.” Read literally, the provision extends to individuals wherever they are taken in to custody or brought under the control of the United States, who fit within our definition of an enemy combatant in the
conflict against al Qaeda and its affiliates — including those arrested in the U.S. by first responders in law enforcement. This would include an individual who, in the midst of an interrogation by an FBI or TSA officer at an airport, admits he is part of Al Qaeda. Must the agent stop a very revealing and productive interrogation and go call the Army to take the suspect away?

On top of all that, the provision adds that the individual must be a member or part of Al Qaeda or an "affiliated entity." While we use the phrase "Al Qaeda and its affiliates" publicly to describe the contours of the conflict in non-legal terms, the term "affiliated entity" has no accepted legal meaning and has never been tested in court. Likewise, the phrase in the bill "a participant in the course of planning or carrying out an attack against the United States" — has never been tested in court.

For this and future Administrations, we will oppose efforts to make military detention more controversial, and restrict the Executive Branch's flexibility to pursue our counterterrorism mission. The Executive Branch, regardless of the administration in power, needs the flexibility, case-by-case, to make well-informed decisions about the best way to capture, detain and bring to justice suspected terrorists.

The conflict against Al Qaeda is complex and multi-faceted. Congress must be careful not to micromanage, complicate and impose across-the-board limits on our options. Both the Congress and the Executive Branch must be careful not to impose rules that make military detention more controversial, not less.

I have spoken today about ways to legally solidify and improve armed conflict, not end it. This should not be the natural order of things. But war is sometimes necessary to secure peace. You heard me describe the tragic but heroic story of a young naval officer who lost his eyesight to an IED. Martin Luther King, the man for whom we dedicated a national memorial on Sunday, said that in the end, an eye for an eye leaves everybody blind. No matter how much longer this conflict will go on, we should all continue to believe that the arc of the human experience on Earth is long, but it bends toward peace.

Thank you for listening.
STATEMENT FOR THE RECORD BY

ROBERT LITT
GENERAL COUNSEL
OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS AND
SUBCOMMITTEE ON INTELLIGENCE COMMUNITY MANAGEMENT

OCTOBER 27, 2009

Chairwoman Schakowsky, Chairwoman Eshoo, Ranking Member Miller, Ranking Member Myrick, and Members of the Committee: thank you for inviting me to speak to you today about the Congressional notification process and the practices and procedures in place throughout the Intelligence Community to help ensure that the Congressional intelligence committees are kept fully and currently informed of significant intelligence activities.

Congressional oversight of the Intelligence Community is critical because of the importance of intelligence in protecting our national security, the power of the tools given to the Intelligence Community and their potential risks to privacy, civil liberties, and foreign relations if used improperly, and the necessarily secret nature of much of what the Intelligence Community does. Congress and the President have established reporting and oversight procedures that balance Congress’ oversight responsibility with the need to protect our nation’s most sensitive information. This oversight, conducted by the intelligence committees through dedicated Members and a cadre of knowledgeable and experienced staff, is a valuable contribution to improving the quality of intelligence and the effective, efficient operation of the Intelligence Community. In addition, robust oversight helps secure the trust of both Congress and the public
in the Intelligence Community. I believe that the Intelligence Community benefits from input from Members of Congress because they bring a different perspective on some of the difficult issues we confront. The value of their input would be limited if the intelligence committees were not “fully and currently informed” of significant intelligence activities.

The Intelligence Community takes seriously its obligation to keep the intelligence committees informed both of the information it needs to conduct intelligence oversight and of national intelligence to inform Congress in its policy-making role. Indeed, Director Blair has repeatedly emphasized the importance of timely congressional notification, and the notification process is subject to the DNI's continued supervision and oversight. Let me give you some statistics: Since the beginning of the 111th Congress, the Intelligence Community has provided the HPSCI over 500 written Congressional notifications, given approximately 800 briefings, and participated in 20 HPSCI hearings. It has provided the HPSCI several thousand intelligence assessments, reports, and written products on intelligence programs. In addition, the Intelligence Community makes a significant amount of information available to Congress via our classified internet platform called ‘CapNet’, including daily classified intelligence updates on-line from the National Counterterrorism Center, State/INR, the CIA, DIA, NGA and the Office of the DNI among others. In short, the Intelligence Community is working hard to make sure that the intelligence oversight committees have timely and accurate intelligence information to inform policy and enable them to conduct oversight.

This is in accord with our statutory responsibility. To ensure that the intelligence committees are kept “fully and currently informed,” the National Security Act requires the Director of National Intelligence and the heads of all departments and agencies with intelligence
components to notify the committees of intelligence activities, including significant anticipated intelligence activities, significant intelligence failures, and covert actions. This obligation must be exercised “consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive sources and methods or other exceptionally sensitive matters,” which provides the DNI and the heads of departments and agencies a degree of latitude in deciding when and how to bring extremely sensitive matters to the committees’ attention.

In addition, the DNI has a statutory obligation to ensure that all Intelligence Community elements comply with the Constitution and laws of the United States, including the Congressional notification requirements of Title V of the National Security Act. DNI Blair takes seriously his responsibility to ensure that Congress has the information it needs to conduct oversight of the Intelligence Community, and I want to tell you a little bit about what Director Blair and his predecessors have done to carry out that obligation.

In January 2006, an Intelligence Community Policy Memorandum (ICPM) entitled “Reporting of Intelligence Activities to Congress” was issued. That Memorandum, which is binding on all elements of the Intelligence Community, provides guidance about the requirements of notification to the committees. In March of this year, Director Blair issued a memorandum to the heads of all the Intelligence Community elements reaffirming the ICPM and directing that notification of any significant intelligence activity be provided to the intelligence committees within 14 days.

In addition, beginning last summer, Director Blair directed a comprehensive review of the Congressional notification policies and procedures throughout the Intelligence Community.
This review examined whether all Intelligence Community elements were in compliance with Congressional notification obligations and had policies and procedures in place to ensure the intelligence committees would be kept fully and currently informed going forward. At the conclusion of this review, the DNI suggested that each element compare its current policies and procedures to a number of suggested "best practices" and make any necessary changes. These best practices include:

- A process for the head of each IC element informally to canvass his or her leadership regularly for matters requiring Congressional notification. In turn, senior leadership personnel should canvass their offices or components.

- Training and education programs to ensure that personnel understand the duty to identify and put forward matters requiring Congressional notification.

- Written procedures that both establish the obligations related to Congressional notification and outline the internal processes to ensure that significant intelligence activities are identified and reported in a timely fashion, including specifying a point of contact that will have responsibility for ensuring that notifications are timely made.

The DNI will continue to review compliance with Congressional notification requirements by the entire Intelligence Community and, if necessary, will evaluate whether to modify the ICPM.
Intelligence Community elements differ in size, structure, and mission. Some elements, such as the CIA, are large and conduct extensive operations; others are small and purely analytical. Accordingly, there is no need for a detailed "one size fits all" policy on Congressional notification for the entire Intelligence Community. For example, a dollar threshold for "significance" might be very different for the State Department’s Bureau of Intelligence and Research, compared to the National Reconnaissance Office. Rather, different elements should adopt procedures that are adapted to their particular situations. It is essential, however, that each element have standards and procedures that are designed to ensure, to as great an extent as possible, that significant intelligence matters are identified according to a clear and consistent standard, and that such matters are promptly and fully reported to the intelligence committees.

In summary, intelligence oversight is critical to the successful operation of the Intelligence Community, but this oversight can only be effective if the Intelligence Community keeps the intelligence committees fully and currently informed of intelligence activities. The DNI is committed to working with the intelligence committees and the Intelligence Community to address this important issue.

I appreciate having the opportunity to come before this subcommittee today, and I look forward to responding to your questions. However, as you know, because the facts surrounding particular notifications are often classified, I will not be able to discuss specific or hypothetical examples in this open session.
NOMINATION OF ROBERT S. LITT TO BE GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND NOMINATION OF STEPHEN W. PRESTON TO BE GENERAL COUNSEL, CENTRAL INTELLIGENCE AGENCY

HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
OF THE
UNITED STATES SENATE
ONE HUNDRED ELEVENTH CONGRESS
FIRST SESSION
MAY 21, 2009

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE
56-455 PDF WASHINGTON : 2010
Keeping the Intelligence Committee Fully and Currently Informed

QUESTION 1:

Section 502 of the National Security Act of 1947 provides that the obligation to keep the congressional intelligence committees fully and currently informed of all intelligence activities applies to the Director of National Intelligence and to the heads of all departments, agencies, and other entities of the United States Government involved in intelligence activities. What is your understanding of the standard for meaningful compliance with this obligation of the Director of National Intelligence and the heads of all departments, agencies and other entities of the United States Government involved in intelligence activities to keep the congressional intelligence committees, including all their Members, fully and currently informed of intelligence activities? Under what circumstances is it appropriate to brief the Chairman and Vice Chairman and not the full committee membership?

ANSWER: I believe that Congressional oversight is particularly important in the area of intelligence, because of the importance of intelligence to protecting our national security, the power of the tools given to the Intelligence Community and their potential risks to privacy and civil liberties if used improperly, and the necessarily secret nature of much of what the Intelligence Community does. As the question notes, Section 502 of the National Security Act requires the Director of National Intelligence, and the heads of all departments and agencies with intelligence components, to keep the two intelligence committees "fully and currently informed" of all U.S. intelligence activities (excepting covert actions that are covered in section 502), including "significant anticipated intelligence activities" and "significant intelligence failures." By its terms, section 502 contemplates that the committees will be notified of all significant intelligence activities before they are undertaken, and section 503 imposes a similar requirement for covert actions.

Director Blair has emphasized the importance of timely and complete congressional notification. On March 24, 2009, he issued a memorandum to the heads of all components of the Intelligence Community reminding them of their obligation in this regard and directing that they review their internal procedures to ensure full and timely compliance. Like Director Blair, I believe that congressional notification must be timely to be effective, and I anticipate that, if confirmed, my responsibilities as General Counsel will include assisting him in ensuring that the entire Intelligence Community carries out this critical responsibility.

Although Section 502 provides that congressional notification must be made "to the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive sources and methods or other exceptionally sensitive matters,"
believe that this phrase does not limit the obligation to keep the intelligence committees “fully informed” but rather provides the DNI a degree of latitude in deciding how he will bring extremely sensitive matters to the committees’ attention. In certain rare circumstances, I believe it could be appropriate to brief the Chairman and Vice Chairman of the intelligence committees on particularly sensitive matters. Limited notification should be undertaken only in the most exceptional circumstances, by analogy to the provision of Section 503 that permits limited briefing on covert actions “to meet extraordinary circumstances affecting the vital interests of the United States.” Even in those circumstances, however, I expect that the DNI would discuss his concerns about further briefings with the Chairman and Vice Chairman and have an on-going dialogue with them about how and when the full committee membership should be briefed on the matter.

Priorities of the Director of National Intelligence

QUESTION 2:

Have you discussed with the Director of National Intelligence his specific expectations of you, if confirmed as General Counsel, and his expectations of the Office of the General Counsel as a whole? If so, please describe those expectations.

ANSWER: Director Blair and I have had such discussions. He has made clear that his principal expectation is that, if I am confirmed, I as General Counsel and the Office of General Counsel as a whole will be responsible for providing him timely and accurate advice about the law to enable him to exercise his important responsibilities, but also, as any good lawyer should do, for providing counsel and judgment going beyond the technical requirements of the law and dealing with such issues as whether a particular course of action is wise, prudent or appropriate. He also expects that we will not have a narrow focus on the Office of the Director of National Intelligence but would consider the interests of the Intelligence Community as a whole and the national interest. Finally, he has indicated that he expects to have an open door for his General Counsel and expects me promptly to bring to his attention any legal or policy issues that concern me.

More particularly, Director Blair recognizes that the General Counsel has an important role to play in helping to coordinate overlapping responsibilities within the ODNI and within the Intelligence Community as a whole. He particularly mentioned to me his desire that his General Counsel work closely with the Civil Liberties Protection Officer and Inspector General to help him ensure, as he is required to do by Section 102A(3)(a) of the National Security Act, that intelligence activities are carried out in “compliance with the Constitution and laws of the United States.” For example, the critical function of overseeing compliance with Foreign Intelligence
Surveillance Act is shared among a number of different entities, and he expects that the Office of General Counsel would help coordinate that oversight for maximum effectiveness.

The Office of the General Counsel

QUESTION 3:

The Office of the General Counsel of the Office of the Director of National Intelligence has a myriad of roles and responsibilities. What are your expectations for the Office?

ANSWER: My expectations for the office are much the same as the DNI's expectations. I would expect that its lawyers would provide both sound legal advice and wise counsel, and that they would make clear to the recipients of their advice when that advice is legal and when it reflects judgment and policy considerations. I would expect them to work with the various components of the Intelligence Community to try to enable them to take all necessary steps to protect the nation while not hesitating to tell them where the bounds of the law are. I would expect them to keep their focus on the needs of the Intelligence Community and the nation as a whole, and to work cooperatively, rather than adversarially, with the legal counsel to all other components of the intelligence community. Finally, I would expect them to be proactive rather than reactive as much as possible – to maintain the sorts of relationships with the components of the Intelligence Community that would encourage those components to consult with them on an ongoing basis rather than at the last minute when things have gone off the rails.

a. Do you have any preliminary observations on its responsibilities, performance, and effectiveness?

ANSWER: Obviously, my observations on the operations of the Office of General Counsel to date are extremely limited, but they are very favorable. I have been impressed with the competence, experience, knowledge and dedication of the lawyers I have met so far. The office appears to be integrated into the daily routine of the entire ODNI, well respected within ODNI and the larger legal community, and effective.

b. If confirmed, will you seek to make changes in the numbers or qualifications of attorneys in the office, or the operations of the office?

ANSWER: Generally, it has been my experience that it is best to spend some time in a new position or a new office before starting to make decisions about what to change. If confirmed, I will get to know the attorneys and the office better, and evaluate how effective the office is in helping the Director accomplish his statutory responsibilities. Moreover, if confirmed I would
expect to consult with the Intelligence Committees to obtain their views as to the operations of the office. As an initial matter, however, if confirmed I expect that I would continue the practice of having several of the attorneys in the office be detailed from other legal offices in the Community. These detailees provide the DNI General Counsel’s Office a broader Community perspective and a better understanding of the variety of legal issues facing the elements of the Intelligence Community, and when the detailees return to their components they take with them a Community perspective.

QUESTION 4:

Describe your understanding of the responsibilities of the Director of National Intelligence and the General Counsel of the Office of the Director of National Intelligence in reviewing, and providing legal advice on, the work of the Central Intelligence Agency, including covert actions undertaken by the Central Intelligence Agency.

ANSWER: By statute, the Director of the Central Intelligence Agency reports to the Director regarding the activities of the CIA, and the Director of National Intelligence is specifically charged with many responsibilities relating to the CIA. For example, he is responsible for ensuring compliance with the Constitution and laws of the United States by the CIA, monitoring the implementation and execution of the National Intelligence Program (NIP) and keeping the Congress fully and currently informed of intelligence activities and covert actions. If confirmed, I will assist the Director in the execution of these responsibilities by working with the CIA General Counsel to ensure that legal issues and NIP-funded programs, including covert actions, are carefully evaluated and reviewed and, when appropriate, that any unresolved legal issues are referred to the Department of Justice for additional review.

QUESTION 5:

Describe your understanding of the responsibilities of the General Counsel of the Office of the Director of National Intelligence in the process set forth in the President’s Executive Orders of January 22, 2009, with respect to ensuring lawful interrogations, review and disposition of individuals detained at Guantanamo Bay Naval Base and closure of detention facilities, and review of detention policy options.

ANSWER: The Director of National Intelligence has an important role in carrying out each of those Executive Orders. He is Co-Vice Chair of the Special Interagency Task Force on Interrogation and Transfer Policies established by E.O. 13491, a participant in the detainee review process established by E.O. 13492, and a member of the Special Interagency Task Force on Detainee Disposition established by E.O. 13493. The General Counsel’s role is to provide
legal advice and counsel to the Director and those officials he has designated to assist him with the implementation of these Executive Orders. The Executive Orders raise important and complex legal and policy issues and it is my understanding that the Office of General Counsel has been working closely with ODNI officials and the Intelligence Community on them.

**QUESTION 6:**

Explain your understanding of the role of the General Counsel of the Office of the Director of National Intelligence in resolving conflicting legal interpretations within the Intelligence Community.

**ANSWER:** By virtue of its relationship with the entire Intelligence Community, the General Counsel's Office is well positioned to identify conflicting legal interpretations within the Community. Because the General Counsel does not have decisional authority to resolve such conflicts, if there are conflicting legal views on an issue, I would bring the relevant general counsels together to discuss the issues and attempt to resolve any differing opinions. I would also involve, as appropriate, the experienced attorneys at the National Security Division and the Office of Legal Counsel at the Department of Justice. This process would correspond to the provision of Section 102A(4) of the National Security Act, which charges the Director with ensuring compliance with the Constitution and laws, but generally "through the host executive departments" that contain elements of the Community.

I have worked in the past with several of the Intelligence Community general counsels, or lawyers on their staff, as well as many of the senior attorneys and officials at the Department of Justice, and I would expect that through this cooperative process we could resolve the great majority of legal issues. However, if we are unable to do so, either the General Counsel of the ODNI or any of the other general counsels could refer a legal question to the Department of Justice. Even in that case, I would expect that the Office of General Counsel of ODNI would be involved in the Department of Justice's decision-making process.

**Guidelines under Executive Order 12333**

**QUESTION 7:**

One of the fundamental documents governing the activities of the intelligence Community is Executive Order 12333. Under Executive Order 12333, as amended in July 2008, there are requirements for Attorney-General approved guidelines. For each of the following requirements, describe the principal matters to be addressed by each of the required Attorney General-approved guidelines or procedures, the main issues you believe need to be resolved in addressing these
guidelines or procedures, and your understanding of the schedule and priorities for completing them (or indicate whether the existing named guidelines or procedures are deemed sufficient)

ANSWER: In general, I understand that the General Counsel of the ODNI plays a role in determining the schedule and priorities for drafting required guidelines and procedures. If confirmed, I expect to be involved in that prioritization process as well as the substantive process of developing the actual guidelines.

a. Guidelines under section 1.3(a)(2) for how information or intelligence is provided to, or accessed by, and used or shared by the Intelligence Community, except for information excluded by law, by the President, or by the Attorney General acting under presidential order in accordance with section 1.5(a).

ANSWER: I would expect these guidelines to address a variety of legal issues and privacy protections in order that information collected by Federal Government agencies outside the Intelligence Community can be shared with the Intelligence Community to the greatest extent possible consistent with protecting the privacy, civil liberties, and statutory rights of U.S. persons. (It is my understanding that intelligence and information-sharing within the Intelligence Community is governed by section 1.3(b)(9)(B) of the Order, and guidelines governing this information sharing are contained in ICD 501, issued in January of this year.) Much of the information collected by other Federal Government agencies is protected by various laws, such as the Privacy Act, the Bank Secrecy Act, etc., and it could contain a great deal of information about U.S. Persons. Whether the information can be accessed by the Community, who within the Community can access the information, under what conditions it can be accessed, requirements for handling information related to U.S. persons, and restrictions on how the information can be further used and shared within the Intelligence Community all need to be addressed in the guidelines.

b. Procedures under section 1.3(b)(18) for implementing and monitoring responsiveness to the advisory tasking authority of the Director of National Intelligence for collection and analysis directed to departments and other U.S. entities that are not elements of the Intelligence Community.

ANSWER: It is my understanding that advisory tasking is a process whereby the Director of National Intelligence asks a Federal Government agency that is not part of the Intelligence Community to collect information that is relevant to national intelligence. I would expect guidelines for advisory tasking to focus on the legal authorities that a non-intelligence agency could or should use to collect national intelligence information for the Intelligence Community. All collection activities would need to be consistent with the responding agency’s legal authorities and would need to protect appropriately the privacy and civil liberties of Americans.
Section 1.5(d) of Executive Order 12333 also provides that the heads of departments or agencies shall respond to advisory taskings "to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency." This provision allows responding departments or agencies to issue policies regarding how a particular department or agency would respond to these advisory taskings.

c. Procedures under section 1.6(g) governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if the elements of the IC involved have intelligence responsibilities for foreign or domestic criminal drug production and trafficking.

ANSWER: This section of the Executive Order is directed to the heads of Intelligence Community elements and tells them to participate in the development of these procedures. Under the revised Order, I believe the procedures for the "production and dissemination" of information or intelligence would be covered by the guidelines under section 1.3(a)(2) of the Executive Order, which is discussed in my answer to question 7a, above, and that the relevant Intelligence Community elements would participate in the development of these guidelines.

d. Regulations under section 1.7(g)(1) for collection, analysis, production and intelligence by intelligence elements of the FBI of foreign intelligence and counterintelligence to support national and departmental missions.

ANSWER: The new procedures for the FBI called for by section 1.7(g)(1) were signed by the Attorney General in the fall of 2008, after consultation with the Director of National Intelligence. It is my understanding that they were drafted before the changes to Executive Order 12333 and that the only thing that was affected by the signing of the new Order was the addition of the requirement to consult with the DNI before the Attorney General could approve the procedures, a requirement that was complied with. Both the Acting General Counsel of ODNI and the Civil Liberties Protection Officer tell me that they were actively engaged in reviewing these new procedures before they were signed last fall.

e. Procedures under section 2.3 on the collection, retention, and dissemination of United States person information and on the dissemination of information derived from signals intelligence to enable an Intelligence Community element to determine where the information is relevant to its responsibilities.

ANSWER: The requirement that elements of the Intelligence Community have procedures approved by the Attorney General under section 2.3 for the collection, retention, and dissemination of U.S. person information is unchanged from the prior version of Executive Order 12333, except for the new requirement that the Attorney General consult with the Director
of National Intelligence before approving any new guidelines. In addition, section 2.3 of the new Executive Order, unlike the prior version, permits information derived from signals intelligence to be disseminated to Intelligence Community elements for the purpose of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, but only in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

All Intelligence Community elements are required to operate under so-called “U.S. person rules” when collecting, retaining, or disseminating information regarding U.S. persons. All of the established elements of the Community have had these guidelines in place for years and those guidelines remain in effect, in accordance with section 3.3 of the amended E.O. 12333. I understand that several of the newer elements of the Intelligence Community, such as the ODNI, DHS Intelligence & Analysis, and the Coast Guard intelligence element have drafted U.S. person rules and are currently coordinating their guidelines with the Department of Justice and the ODNI. A few other elements are also updating or revising their U.S. person rules. If confirmed, I expect to be actively involved in this process. I understand that there is an effort to harmonize these guidelines across the Intelligence Community to as great an extent as possible, given the varying missions and requirements of the different components of the Intelligence Community. This project certainly seems desirable, particularly as we move to a more integrated Intelligence Community with ever greater information-sharing.

f. Procedures under section 2.4 on the use of intelligence collection techniques to ensure that the Intelligence Community uses the least intrusive techniques feasible within the U.S. or directed at U.S. persons abroad.

g. Procedures under section 2.9 on undisclosed participation in any organization in the United States by anyone acting on behalf of an IC element.

ANSWER: The guidelines discussed in my answer to question 7e also include the procedures regarding the requirement for the use of least intrusive techniques and the procedures for undisclosed participation in organizations. These provisions of Executive Order 12333 are unchanged from the prior version of the order, except for the addition of a requirement for the Attorney General to consult the Director of National Intelligence before approving guidelines for use of these procedures. If confirmed, I intend to play an active role in that consultation process.
Implementation of the FISA Amendments Act of 2008

QUESTION 3:

Under section 702 of the Foreign Intelligence Surveillance Act, as added by the FISA Amendments Act of 2008 (FISA Amendments Act), the Attorney General and the DNI may authorize jointly, for a period up to one year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information. The FISA Amendments Act was signed into law in July 2008. Thus, the process for one or more new annual authorizations may occur at some time proximate to the first anniversary of the FISA Amendments Act and annually thereafter. The FISA Amendments Act also provide for semiannual or annual assessments and reviews, as described in section 702(f) of FISA.

a. Describe your understanding of the matters that the Attorney General and DNI, with the assistance of the General Counsel of the Office of the DNI (GC/ODNI), should evaluate in order to determine, on the basis of the first year’s experience under the FISA Amendments Act (and annually thereafter), whether there should be revisions in the substance or implementation of (1) targeting procedures, (2) minimization procedures, and (3) guidelines required by the FISA Amendments Act, in order to ensure both their effectiveness and their compliance with any applicable constitutional or statutory requirements.

ANSWER: Under the FISA Amendments Act, as under other statutes and Executive Order 12333, the Intelligence Community has the responsibility both to protect the nation from foreign threats and to protect the civil liberties of Americans. At this point, of course, I do not have knowledge of the classified details of how the Intelligence Community has implemented the FISA Amendments Act. However, section 702(f) of the Act requires the Director of National Intelligence and the Attorney General jointly to conduct semi-annual assessments of compliance with the targeting and minimization procedures adopted in accordance with sections 702(d) and (e), and with the guidelines adopted under section 702(f) to ensure that applications for court orders are properly filed and that the substantive limitations of section 702(b) are complied with. At its core, this assessment is concerned with ensuring that the targets of surveillance under section 702 are really in a foreign country and are not U.S. persons, and that the privacy and civil liberties interests of U.S. persons who may be in communication with the target are protected.

It is my understanding that the Office of General Counsel participates in these semi-annual reviews and other reviews required by FISA. I would expect that the information obtained from these reviews would serve as the basis for evaluating whether changes are required to the targeting or minimization procedures or to the guidelines.
b. Describe how the semiannual or annual assessments and reviews required by the FISA Amendments Act should be integrated, both in substance and timing, into the process by which the Attorney General and DNI consider whether there should be revisions for the next annual authorization or authorizations under the FISA Amendments Act, including in applicable targeting and minimization procedures and guidelines.

ANSWER: Without a detailed knowledge of the implementation of the FISA Amendments Act it would be premature for me to speculate on the appropriate timing or substance of the assessments and reviews required by the statute. However, as noted above, the data obtained from the reviews and assessments should inform any reauthorizations under the Act.

c. In addition to the matters described in the FISA Amendments Act for semiannual or annual assessment or review, are there additional matters that should be evaluated periodically by the Attorney General or the DNI to improve and ensure the lawful and effective administration of the FISA Amendments Act?

ANSWER: It is also premature for me to comment on additional matters that should be reviewed to improve oversight of the FISA Amendments Act without a better understanding of the precise manner in which the authorities granted by the Act have been used and in which the existing oversight and implementation authorities have been employed. However, if confirmed, I look forward to discussing the issue with the Director, the Attorney General, relevant officials of the Intelligence Community, and the Congress.

QUESTION 9:

Title III of the FISA Amendments Act of 2008 provides for a comprehensive report by certain inspectors general on the President’s Surveillance Program during the period beginning on September 11, 2001 and ending January 17, 2001. The final report is to be submitted, within one year of the signing of the law in July 2008, in unclassified form but may include a classified annex.

a. Describe your understanding of the purpose of a public report.

Answer: I believe that the report will provide an important mechanism for ensuring that the facts about this program are available to Congress and the American people, consistent with the protection of intelligence sources and methods. Because the FISA Amendments Act provides for the dismissal of ongoing litigation related to these activities, this report will help to ensure appropriate accountability for the program.
b. Describe the responsibility that you anticipate that the GC/ODNI will have in recommending what should be declassified and the standards that should be applied to that determination.

**ANSWER:** In general, section 1.3(b)(9) of Executive Order 12333 gives the Director of National Intelligence considerable authority over the classification and declassification process for information classified by the Intelligence Community. Transparency into the workings of the government is vital and I believe information that is of interest to the public should be made publicly available to the greatest extent possible. However, balancing that public interest with national security concerns is a difficult challenge. Executive Order 12958 requires that information be declassified when it no longer meets the standards for classification, and also contemplates that at times the public interest in the disclosure of certain information will outweigh the need to protect it. Certainly there are times when information that is of interest to the public can be disclosed without revealing truly sensitive intelligence sources and methods.

I expect that the unclassified report required by the FISA Amendments Act will be a good example of the balancing required in this difficult area and I would expect the General Counsel of the ODNI to play an important role in striking the proper balance in this context.

**December 2009 Sunset of Three FISA Provisions**

**QUESTION 10:**

Three FISA provisions—lone wolf coverage, roving wiretaps, and orders for documents—sunset on December 31, 2009.

a. In your view, what evidence and issues should be considered by the Administration and by Congress in the consideration of whether to modify these provisions and either extend the sunsets or make the provisions, with or without amendments, permanent?

**ANSWER:** As a general matter, I think that the experience of the government in executing these authorities, the value of the information obtained, the degree of intrusion upon civil liberties, and the extent of the continued need for these authorities would all be relevant factors to consider. Without knowing precisely how these authorities have been implemented by the government, I cannot comment more specifically, but if confirmed I expect that I will work with the Congress in evaluating these provisions.
b. Are there any benefits, in your view, in aligning the sunset of these provisions with the sunset under the FISA Amendments Act of 2008 for Title VII of FISA on procedures regarding persons outside of the United States?

**ANSWER:** Again, without knowing precisely how the authorities have been implemented, it is difficult to assess the impact of aligning the sunsets of these provisions.

**Declassification of FISA Opinions**

**QUESTION 11:**

At the end of last year, the FISA Court of Review released to the public a redacted version of its most recent opinion. What are your views regarding the issues to be considered in creating a regular process under which important rulings of law and key decisions of the FISA Court and the FISA Court of Review could be publicly released in an unclassified form?

**Answer:** Balancing the public interest with national security concerns always presents a difficult challenge. There is a public interest to be served in the release of important rulings of law and key decisions of the FISA Court and the FISA Court of Review, including providing a better understanding of the Court's decision-making process and permitting informed public participation in debate over issues relating to FISA. However, these are unique courts whose entire docket relates to the collection of foreign intelligence. Release of these opinions has the potential to expose details of critical intelligence operations, sources, and methods. In my view, the Intelligence Community and the Department of Justice should identify opinions of legal significance the release of which would serve the public interest, and work with the Court to consider release to the extent it can be done in a manner that protects national security information and intelligence activities.

**Evaluation of Office of the Director of National Intelligence**

**QUESTION 12:**

Members of the Committee have expressed concern that the ODNI does not have all of the legal authorities necessary to fulfill congressional expectations for the office. Do you have any preliminary observations on strengths or weaknesses of the authorities of the Office with respect to a successful mission of the ODNI? If so, please describe.
ANSWER: I have not yet had the opportunity to observe the operation of the Office of the Director of National Intelligence and therefore do not have any informed observations on the strengths or weaknesses of its authorities. The Office of the Director of National Intelligence is unlike any other organization in the Federal Government, in that it has responsibilities over Intelligence Community elements that reside in six independent Departments and thus remain accountable to the heads of those Departments as well as to the Director. This arrangement clearly has the potential to complicate the job of the Director. Whether the ODNI has all of the authorities necessary to integrate and lead the Intelligence Community is something that will require further study and experience working under the current authorities. If confirmed, I pledge to work with the Committee during the annual Intelligence Authorization process on legislation to implement any additional authorities that may be necessary for the ODNI to carry out its mission.

Pending Legislation

QUESTION 13:

The Senate and House of Representatives have considered legislation over the course of several Congresses on subjects such as providing conditions for the federally compelled disclosure of information by certain persons connected with the news media, the state secrets privilege, and whistleblower protections. In your view, what evidence and issues should be considered by the Administration and by Congress in the consideration of whether legislation on these subjects should be enacted? Please discuss each subject separately.

ANSWER: Each of these legislative proposals shares a common goal—striking an appropriate balance between ensuring transparency and openness in government and protecting the national security. From my current vantage point, it appears that the evidence and issues that the Administration and Congress should consider with regard to such legislation are similar. For example, section 102A(c)(1) of the National Security Act requires the Director of National Intelligence to "protect intelligence sources and methods from unauthorized disclosure," a responsibility shared by everyone who has access to classified information. Accordingly, both Congress and the Administration must assess whether any legislative proposal would put intelligence sources and methods at risk or could result in the unauthorized disclosure of classified information. For example, we should jointly consider whether the legislation would encourage or prevent leaks of classified information. Similarly, both Congress and the Administration should assess whether the legislation respects the President's constitutional obligation to protect and control classified information, and whether it provides appropriate deference to Executive Branch determinations that the disclosure of classified information has or will cause damage to the national security. In addition, Congress and the Administration should assess whether the legislation would impede the effective operations of the Intelligence Community.
At the same time, Congress and the Administration need to evaluate whether existing laws and procedures have hindered the free flow of information to the public or the Congress or have resulted in unjust results in particular cases, and whether these legislative proposals would effectively remedy any such problems. Finally, as these proposals share a common goal, they should be evaluated as a collective whole rather than in isolation.

**Cyber Security**

**QUESTION 14:**

The Bush Administration launched a major initiative to improve government cyber security, the Comprehensive National Cybersecurity Initiative (CNCI), with a prominent role for the Intelligence Community. The Obama Administration has undertaken a 60-day review of cyber security.

a. What are the major legal, privacy and civil liberties issues concerning the CNCI, or successor, that you believe should be addressed?

**ANSWER:** Computer security has been a particular concern of mine since my time at the Justice Department. Our nation's cybersecurity policy addresses a wide range of issues that cut across multiple mission areas and therefore multiple legal authorities. We are faced with adversaries who have the ability to infect our supply chain with maliciously modified hardware and software, to hack remotely into our networks, and to take advantage of insiders to steal, alter, or destroy information and control critical infrastructure systems. Moreover, a pressing but under-appreciated privacy issue is that our sensitive data, including corporate intellectual property, government secrets, and U.S. person data held by government and private industry alike, is not only vulnerable but is actually being stolen by criminal organizations and foreign nations on a daily basis and almost at will.

To guard against exploitation of these vulnerabilities, our government must bring to bear all of its capabilities, including those within the Intelligence Community, to ensure the privacy and security of our global information and communications infrastructure. This will require a focus on intrusion detection and prevention monitoring, information-sharing policies, data accuracy, and analysis. At the same time, we must remain vigilant to ensure that the use of government authorities meant to detect our adversaries and thwart their efforts complies strictly with the Constitution and the law. If confirmed, I will work closely with the ODNI Civil Liberties Protection Officer to ensure that there is adequate oversight of these authorities.
b. What overarching guidelines for the Intelligence Community do you believe should be in place with respect to the implementation of any successor to the CNCl?

**ANSWER:** I am not fully familiar with the CNCl or the Administration's ongoing study of cybersecurity, the recommendations of which have not yet been made public. If confirmed, I will take an in-depth look into appropriate, overarching guidelines. In doing so, I expect to work closely with the Civil Liberties Protection Officer, as well as the Department of Justice and the elements of the Intelligence Community.

**Executive Branch Oversight of Intelligence Activities**

**QUESTION 15:**

Are there improvements, in terms of resources, methodology, and objectives that you believe should be considered concerning Executive Branch oversight of the intelligence activities of the United States Government?

**ANSWER:** Intelligence oversight is an essential tool to achieve the important goal of balancing the protection of our civil liberties with the protection of our national security. As the chief legal officer for the Office of the Director of National Intelligence, the General Counsel has the responsibility to assist the Director in carrying out his statutory authority under section 102A(3)(4) of the National Security Act to "ensure compliance with the Constitutions and laws of the United States." The authorities granted to the Intelligence Community are of necessity powerful ones, and the public needs to be reassured of our continued commitment to compliance with the important limitations imposed by our laws. If confirmed as General Counsel, I will assist the Director in using intelligence oversight to achieve this goal.

It is premature for me to comment on specific improvements that I might recommend in the resources, methodology and objectives of this oversight. However, if confirmed, I would expect that ensuring the Intelligence Community provides timely, accurate, and thorough intelligence oversight reporting will remain a priority for the Office of General Counsel. Moreover, if confirmed, I will consult with my staff, with the General Counsels of all elements of the Intelligence Community, and with Department General Counsels, to determine whether any improvements are needed in intelligence oversight.
Relationship with the Other Officials of the Intelligence Community

QUESTION 16:

What should be the relationship of the General Counsel of the Office of the Director of National Intelligence with respect to the following officials of the Intelligence Community:

a. General Counsel, Central Intelligence Agency

ANSWER: Section 102A(4)(d) of the National Security Act, concerning the responsibility of the Director of National Intelligence to "ensure compliance with the Constitution and laws of the United States" by the Intelligence Community, recognizes the special relationship that the Central Intelligence Agency has to the DNI, by giving him direct responsibility to ensure compliance "by the Central Intelligence Agency" while providing that he should ensure compliance by other elements of the Community "through the host executive departments" containing those elements. The statute thus clearly contemplates a very close working relationship between two agencies and, by extension, their General Counsels. I have known Steve Preston for many years and have great respect for his abilities and judgment, and if we are both confirmed, I look forward to a close and open relationship with him on a wide range of issues.

b. Assistant Attorney General for National Security, Department of Justice

ANSWER: The position of Assistant Attorney General for National Security did not exist during my time at the Department of Justice, but if confirmed, I look forward to the opportunity to work closely with David Kris, whom I have known since we worked together at the Department. Although the National Security Division is not part of the Intelligence Community, its responsibilities obviously touch on many matters of significance to the Community. For example, the General Counsel of ODN and the Assistant Attorney General for National Security must routinely work together to assist the Director and the Attorney General in their respective authorization and oversight roles under the FISA Amendments Act. The recent Executive Orders on rendition, detention, and interrogation also require a close working relationship between the offices. The General Counsel's Office and the National Security Division have implemented a program to have a detailer from the National Security Division at the ODN General Counsel's office. I understand that this arrangement has been tremendously valuable to both agencies.

c. Inspector General, Office of the DNI

(see below)
d. Civil Liberties and Privacy Officer, Office of the DNI

ANSWER: I believe that it is essential that the ODNI General Counsel have a close working relationship with both the ODNI Inspector General and the Civil Liberties Protection Officer. If confirmed, I would expect my interactions with these officers to be both formal and informal. On the one hand, because the oversight roles that the three offices fulfill for the ODNI and for the Intelligence Community are very similar, we will need formal processes to coordinate our roles to make sure that we are as effective as possible while minimizing unnecessary duplication. On the other hand, conflict and duplication can best be minimized if the three officers consult informally and work together whenever possible. The three offices have many similar, but distinct, responsibilities and approach those responsibilities from different perspectives. This provides a unique opportunity for collaboration that should allow each of us to get a more comprehensive picture of any problem and also of possible solutions. I have known the new ODNI Inspector General, Roslyn Mazer, for many years and served with her in the Department of Justice; I met Alex Joel, the Civil Liberties Protection Officer, during my preparation for the hearings, and was impressed with his energy and abilities. If confirmed, I look forward to working closely with both of them.

Professional Experience

QUESTION 17:

For each of the following, describe specifically how your experiences will enable you to serve effectively as the General Counsel for the Office of the Director of National Intelligence.

Include within each response a description of issues relating to the position that you can identify based on these experiences.

a. Partner, Arnold and Porter LLP

ANSWER: At Arnold & Porter I have represented several employees of the Central Intelligence Agency on matters arising out of their employment, some of which are classified, and have dealt extensively on those matters with the CIA and its Office of General Counsel and Office of Inspector General. These have given me familiarity not only with the particular substantive matters that were the subject of the representations but also with personnel and administrative matters that I believe are relevant to the duties of the General Counsel for the Office of the Director of National Intelligence.
In addition I have represented two clients in criminal matters that related to the intelligence community, one of which involved extensive litigation under the Classified Information Procedures Act (CIPA). It is my understanding that dealing with CIPA issues in individual cases and on a policy basis is part of the responsibility of the Office of General Counsel.

Finally, while at Arnold & Porter I have remained actively involved in matters relating to intelligence policy and national security, through bar associations and speaking and writing engagements. I have also benefited greatly from the knowledge and wisdom of my partner Jeff Smith in this regard.

b. Principal Associate Deputy Attorney General, Department of Justice

ANSWER: See below.

c. Deputy Assistant Attorney General, Criminal Division, Department of Justice

ANSWER: As Deputy Assistant Attorney General in the Criminal Division, and as Principal Associate Deputy Attorney General, I interacted regularly with components of the Intelligence Community on such matters as crimes reports, requests for opinions on the legality of proposed conduct, FISA applications, criminal investigations that involved classified information (including criminal investigations relating to al Qaeda), and covert actions. As a result I acquired a working familiarity with some of the legal authorities governing the Intelligence Community, and how those authorities operate in practice.

I also dealt extensively with matters relating to computer security, privacy and electronic surveillance, which are critical to the effective functioning of the Intelligence Community and to protection of our national security. I helped to create and stand up the Department's Computer Crime and Intellectual Property Section and served as the Department's representative on matters relating to encryption and the Communications Assistance to Law Enforcement Act (CALEA).

In addition, I developed personal relationships with other Intelligence Community lawyers that will be important, if I am confirmed, in enabling me to perform the coordinative function for the General Counsel for the Office of the Director of National Intelligence for the Intelligence legal community.

More generally, my experience in the Department of Justice familiarized me with the operation of the interagency process, with the mechanisms of congressional oversight, and with the process of developing legislation, all of which will be an important part of my role as General Counsel if I am confirmed. In addition, my years at the Department of Justice gave me valuable experience in managing an office of government lawyers.
d. Special Advisor to the Assistant Secretary of State for European and Canadian Affairs

ANSWER: During my year at the Department of State I was a consumer of intelligence and acquired some understanding of the importance of intelligence to our foreign relations and national security.

e. Assistant U.S. Attorney, Southern District of New York, Department of Justice

ANSWER: One of the important issues that faces the government as a whole, including the General Counsel of the Office of the Director of National Intelligence, is how to handle suspected terrorists who we now have in custody or who may subsequently come into our custody. The President has appointed task forces to analyze these issues and I understand that the Office of General Counsel of ODNI is participating in the work of those task forces. If I am confirmed, I believe that my experience as a prosecutor who has actually investigated and tried criminal cases will be valuable both in helping to make the policy decisions about how our legal system should handle accused terrorists, and in assisting the Intelligence Community in responding to the exigencies of particular cases in the judicial system.

QUESTION 18:

What, if any, conflicts might arise from your private practice if you are confirmed as General Counsel and how would you address these conflicts?

ANSWER: In connection with the nomination process, I have consulted with the Office of Government Ethics and the Office of the Director of National Intelligence's designated agency ethics official to identify potential conflicts of interest. Any potential conflicts of interest will be resolved in accordance with the terms of an ethics agreement that I have entered into with the ODNI's designated agency ethics official and that has been provided to this Committee.

With respect to my current or former clients, I have represented a State Department employee in a criminal matter and currently represent several present and former employees of the CIA in DOI, congressional and IG investigations. In addition, my law firm represents a number of telecommunications and high-tech companies on matters on which I have been consulted from time to time. Some of these matters have been classified. My law firm also was appointed by the United States Court of Appeals for the Fourth Circuit to represent Zacarias Moussaoui on appeal. In 2007-08 I assisted the lawyers who handled the matter by providing legal advice about the criminal law and by participating in moot courts.

Should a conflict arise, in accordance with the terms of my ethics agreement, I will not participate personally and substantially in any particular matter involving specific parties in which a former client of mine is a party or represents a party for a period of one year after I last provided service to that client, unless I am first authorized to participate, pursuant to 5 C.F.R. §
2635.502(d). I also understand that I am required to sign the Ethics Pledge (Executive Order 13490) and that I will be bound by its requirements and restrictions. I am not aware of any potential conflicts of interest not covered under the terms of the ethics agreement or the Ethics Pledge.

Opinions of the Office of Legal Counsel

QUESTION 19:

On April 16, 2009, the Department of Justice released four opinions issued by the Office of Legal Counsel (OLC) for the Acting General Counsel or Senior Deputy General Counsel of the Central Intelligence Agency. With respect to these opinions, issued August 1, 2002, May 30, 2005, and two issued on May 10, 2005:

a. From the information contained in the opinions, what are your views concerning the role of the Office of the General Counsel of the Central Intelligence Agency in providing information to the OLC in this matter, and whether any lessons for the future should be learned from these opinions regarding that role for the General Counsel of the Central Intelligence Agency or any other general counsel of an entity of the Intelligence Community, including the General Counsel of the Office of the Director of National Intelligence?

ANSWER: I am not sufficiently familiar with the full details of the interaction between the General Counsel of the Central Intelligence Agency, the Office of Legal Counsel, and other parts of the Executive Branch to offer any specific comments on their role in the preparation of these opinions. In general, however, from my prior experience in government I know that the Office of Legal Counsel’s work in providing authoritative legal opinions to the Executive Branch depends upon obtaining full and accurate information from any agency that requests its views. In addition, it is my view, as noted above, that an agency general counsel should provide not only technical legal advice to the agency but judgment and policy guidance. I would expect the General Counsel of the ODNI to be involved in any opinions that relate to the Intelligence Community.

b. If confirmed, will you expect to be informed of requests by agencies of the Intelligence Community for opinions from the Office of Legal Counsel?

ANSWER: Yes. However, it is certainly possible that a Department Secretary could independently ask the Department of Justice for a legal opinion. A close working relationship with the National Security Division, the Office of Legal Counsel, and other offices at the
Department of Justice can help ensure that the General Counsel's Office participates in the process of preparing legal opinions that could affect the Intelligence Community.

c. What is your assessment of the legal reasoning and conclusions of each of these four opinions?

ANSWER: These opinions have been withdrawn by the Department of Justice, indicating that their reasoning and conclusions may not be relied upon. In addition, the President has ordered that interrogation techniques be limited to those authorized by the Army Field Manual, and has established a task force, of which the Director of National Intelligence is co-vice chair, to review interrogation policies for the future. If confirmed, I would expect that I would carefully review any proposed interrogation techniques and ensure that any legal opinions that are rendered are based upon a full understanding of the relevant facts and law.
COMMITTEE QUESTIONS FOR THE RECORD
NOMINATIONS OF ROBERT S. LITT AND STEPHEN W. PRESTON
May 26, 2009

Congressional Notification

Mr. Litt and Mr. Preston, in addition to the responses you have already given concerning congressional notifications, please also respond to the following:

• Would you both support, in those circumstances in which the legality of an intelligence activity has been evaluated in a legal opinion of the Department of Justice or of a General Counsel’s Office in the Intelligence Community, providing that opinion to the congressional intelligence committees?

Section 502 of the National Security Act requires that the intelligence committees be kept fully and currently informed of all significant intelligence activities, and as I have stated, I believe that the Intelligence Community will benefit from greater congressional oversight and input into important decisions. In many instances, legal opinions rendered by the Department of Justice may be important to that oversight. If confirmed, I will work to ensure that the committees have the information they need to conduct effective oversight, including relevant legal opinions. In some instances, where applicable privileges may be involved, I will work cooperatively with the committee to find alternative avenues of accommodating congressional oversight interests.

• With respect to the content of limited briefings, what measures would you support to provide for complete records of any such briefings? For example, the establishment of a DNI registry of them? The submission by the DNI or the DCIA of a written statement to the Chairman and Vice Chairman? Non-objection to the creation of a congressional record, through the Committee’s cleared reporter or a recording? Other means?
As Director Blair has said, in the rare cases in which limited briefing is appropriate, such briefings will include a discussion with the Chairman and Vice Chairman of the committee regarding when and how briefing of the full committee membership is appropriate. I believe that this consultation should also include discussion of whether a record of the limited briefing should be prepared and, if so, what type of record would be most appropriate.

- To determine whether there are matters of continuing interest that were briefed to prior committee leaders but not to the current Committee, would you undertake a review of all limited notifications of the past ten years and provide to the Committee a comprehensive list of them?

All such limited notifications are under the purview of the President and I do not believe that the General Counsel of the Office of the Director of National Intelligence has the authority to provide such a list. Going forward, Director Blair has committed to briefing the full membership of the intelligence committees, except in rare exceptional cases, and if confirmed, I will work with the Committee to ensure that it has the information it needs to conduct effective oversight.

- In the limited cases in which notification to a group smaller than the full committees is provided, what is the statutory basis, if any, for limiting the notification to the Gang of Four (the leaders of the two committees) rather than the full Gang of Eight (thereby including the Leaders)?

Section 502 of the National Security Act provides that the intelligence committees must be kept fully and currently informed "(t)o the extent consistent with due regard for the protection from disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters." In rare circumstances, this might authorize briefing of a smaller group, although I believe this should only be done in consultation with the leadership of the intelligence committees.

There is an interest on the Committee, reflected in legislative proposals in our authorization bills, in changing the notification provisions in the National Security Act to ensure that the full Committee is informed.

- Do you think the notification provisions need to be amended?
• Would you work with this Committee in crafting appropriate amendments?

Like Director Blair, I believe that effective Congressional oversight of the intelligence community is extremely important and that the notifications to the committee of significant intelligence activities are essential to that oversight. While the Director may, in rare circumstances, brief a smaller group on particularly sensitive matters, the Director has committed that such briefings will include a discussion regarding how and when the full committee membership should be briefed on the matter. The notification requirements contained in the National Security Act represent a careful compromise between the Executive Branch and the Congress in an area where both have significant constitutional authorities, and I do not think it is prudent to alter this fundamental compact. If confirmed, I intend to have an ongoing dialogue with the committees to discuss how the Intelligence Community, and the Office of General Counsel in particular, can better help the intelligence committees conduct effective oversight, including ways to ensure that the committees are kept fully and currently informed.

The Clients of the National Security Lawyer

Mr. Preston, during the hearing you were asked about your response to the prehearing questions about the unclassified conclusions of the CIA Inspector General's report entitled "Procedures Used in Narcotics Airbridge Denial Program in Peru, 1995-2001" and when it might be appropriate to advise clients not to create discoverable documents during civil litigation or while facing the threat of civil litigation. Please provide written responses to these questions:

• Does the DNI General Counsel have any responsibilities higher than ensuring that the ODNI and all its personnel act in accordance with the law and maintain full and accurate records of their actions?

A primary responsibility of the General Counsel of the Office of the Director of National Intelligence is to assist the Director of National Intelligence in carrying out his statutory responsibility to ensure that all activities of the
Intelligence Community are conducted in compliance with the law, including any laws relating to the creation and maintenance of full and accurate records. As I have previously stated, I also believe that a General Counsel owes his or her client the benefit of "counsel" in addition to legal advice.

- Does the DNI General Counsel have any role in representing personnel in investigations by the Department of Justice or by the DNI Inspector General?

No. The ODNI Office of General Counsel does not represent individuals. Individuals are represented by the Department of Justice, if appropriate, or by private counsel. The Office of General Counsel works with the Department of Justice in appropriate cases to assist the Department in its representation of government personnel.

- What is the General Counsel's role in litigation to redress harm to individuals allegedly caused by ODNI actions? In your view, is the DNI General Counsel another member of the defense team?

The primary role in defending litigation rests with the Department of Justice. The role of the ODNI General Counsel in any such litigation is to represent the Office of the Director of National Intelligence and the Intelligence Community as a whole, in the interest of the American public, and to assist the Department of Justice, as requested.

Mr. Litt, please provide your written responses to the same questions above with respect to the General Counsel of the ODNI, including your answer to the question asked at the hearing concerning who is the "client" of the ODNI General Counsel.

I believe that, if confirmed, my primary client in most cases will be the Office of the Director of National Intelligence, and the Intelligence Community as a whole, in the interest of the American public.
Confirming General Counsels

Mr. Litt and Mr. Preston, Congress chose to require Senate confirmation for both the DNI and CIA General Counsel positions. Mr. Preston was specifically asked about his understanding of the purpose of the establishment of a confirmed General Counsel of the Central Intelligence Agency.

- Mr. Preston, what is your understanding of the purpose of Congress's establishment of a confirmed General Counsel?

- Mr. Litt, what is your understanding of the requirement for Senate confirmation of your position?

I believe that the purpose of ensuring Senate confirmation is twofold: first, so that the Senate is satisfied that the nominee is qualified to perform the duties of the General Counsel, and second, to ensure that the Senate is satisfied that the nominee will be responsive to and cooperative with congressional oversight.

Conflicts

Mr. Litt, you have informed the Committee that you have certain potential conflicts from your representations in private practice and you discussed this issue with Senator Feingold at the hearing.

- What additional information can you place on the public record about the nature of those conflicts, how you will resolve them, and the extent to which they might affect your ability to provide the DNI with legal counsel?

I represent several present and former employees of the Central Intelligence Agency in matters relating to the detention and interrogation of suspected terrorists. By statute, under the rules of ethics and by virtue of my ethics agreement that has been provided to the Committee, I will not participate
personally and substantially in any particular matter involving these clients. I have consulted with the ODNI Designated Agency Ethics Official about the scope of that bar, and while its precise contours will have to be determined on a case-by-case basis, I will not participate in any decisions relating to the possible prosecution or investigation of these individuals nor any decisions that would affect the outcome of such matters, including decisions about similarly situated individuals or offering an opinion with respect to the legal status of particular interrogation procedures that may have been employed in the past that relate to the subject of my representation.

A principal function of the Director of National Intelligence, and by extension the General Counsel of ODNI, is to set forward-looking policies and procedures to ensure compliance by the Intelligence Community with the Constitution and laws of the United States. I do not believe my prior representation will impose any limitations on my ability to participate fully in that process as it relates to detention and interrogation going forward.

These recusals would only affect my ability to provide the DNI with legal counsel in narrow areas related to my prior representation. There will remain a wide variety of issues falling within the responsibilities of the Office of General Counsel that I will be able to participate in fully.

Mr. Preston, in addition to informing the Committee about potential conflicts from your private practice, what information can you place on the public record about those conflicts and their resolution?
Conflicting legal opinions

Mr. Litt, in your responses to the Committee's prehearing questions, you noted that you would work with the CIA General Counsel to ensure that legal issues related to the work of the CIA are reviewed and evaluated. You also indicated that you would work with the general counsels of the various intelligence agencies and with attorneys from the Department of Justice with respect to conflicting legal opinions within the Intelligence Community. You also stated that the DNI General Counsel does not have decisional authority to resolve conflicting legal interpretations in the Intelligence Community.

- Do you think the DNI General Counsel has an independent obligation to assess for the DNI the legality of covert actions and other intelligence programs?

Yes.

- If the Department of Justice were to issue an opinion with which you disagreed from a legal standpoint, how would you counsel the DNI?

If I was unable to resolve the disagreement through discussions with the Department of Justice, I would advise the Director of National Intelligence to raise the issue through appropriate channels, to the President if the situation warrants it.

- Do you think the DNI General Counsel should have decisional authority to resolve conflicting legal views within the Intelligence Community?

The Attorney General is the chief legal officer of the United States Government, and generally speaking, the Department of Justice, and more particularly the Office of Legal Counsel, is charged with resolving disputed legal issues within the Executive Branch. If there is a conflict within the Intelligence Community on a legal issue and the ODNI Office of General Counsel is not able to resolve the conflict, if confirmed I would bring the matter to the attention of the Director and refer the issue to the Department of Justice for resolution if necessary.
Mr. Preston, will you undertake to ensure that the ODNI General Counsel has full awareness of significant legal interpretations of your office?
Attorney General Guidelines

Mr. Litt, in your responses to the Committee's prehearing questions, you noted that you expected Attorney General guidelines on information sharing promulgated pursuant to Executive Order 12333 to protect the privacy, civil liberties and statutory rights of US persons.

Please elaborate. In creating those guidelines, how would you recommend the DNI balance the need for information sharing with the privacy interests of US persons?

I believe that privacy and civil liberties interests should always be considered in tandem with proposals for information-sharing. Privacy and civil liberties are often best protected through legal processes, such as procedural and substantive requirements that must be met before information-sharing is permitted in a particular case. In general, the appropriate level of protection in this context should be determined by balancing the severity of the intrusion and the importance of the information to protecting national security. Greater intrusions upon civil liberties and privacy should generally require more stringent predicates and a higher level of approval; on the other hand, exigent circumstances or grave dangers to national security may warrant more flexible procedures. If confirmed, I would work closely with the Civil Liberties Protection Officer and his office in advising the Director with regard to the information-sharing guidelines promulgated pursuant to Executive Order 12333.

- Are there particular types of records or information about US persons that should never be shared or should this depend on the need for those records?

Some records should rarely be shared, but I am reluctant to say that there is any category of record that should never be shared regardless of the importance to national security. Even information protected by legally recognized privileges can generally be released under appropriate circumstances, such as pursuant to court order or to prevent a serious crime from occurring. However, as described above, the greater the intrusion on personal privacy, the stronger the procedural and substantive protections should be.
Declassification—IG Reports and OLC Opinions

Mr. Litt, the DNI will likely be involved in recommending whether information about both the Terrorist Surveillance Program and CIA’s detention and interrogation program should be declassified, and will likely seek your counsel on those topics. In your responses to the Committee’s prehearing questions, you noted that the public interest in the disclosure of certain information may outweigh the need to protect it.

- In what circumstances do you think disclosure of information is in the public interest?

In general, I believe that information that relates to matters of national interest should be made publicly available to the greatest extent possible and that there should be a presumption of openness, to enable robust and informed public discussion. However, in some instances countervailing interests, such as the privacy of Americans or national security, may overcome the presumption of openness.

- Do you support the recent declassification of the four OLC opinions on CIA’s detention and interrogation program?

Yes.

- Mr. Preston, what are your views on the declassification of the OLC opinions?
Declassification—FISA Court Opinions

Mr. Litt, in your responses to the Committee’s prehearing questions you noted that the Intelligence Community and the Department of Justice should identify FISA court opinions of legal significance whose disclosure would serve the public interest for potential declassification.

• Do you support having a regular, mandated process for review of those opinions and discussion with the FISA court about possible declassification?

I believe that any process for declassification of FISA Court opinions of legal significance should be undertaken in consultation with the Department of Justice and the FISA Court, and must protect national security information. If confirmed, I will work with the Department of Justice, to determine the best way to accomplish the goal of informing the public of significant legal interpretations of FISA.

Pending legislation

Mr. Litt, in response to prehearing questions on legislation relating to federally compelled disclosure of information by persons connected to the news media, the state secrets privilege and whistleblower protections, you noted that the various legislative proposals should be evaluated collectively. You also stated that it was important to consider, among other things whether the legislation “provides appropriate deference to Executive Branch determinations that the disclosure of classified information has or will cause damage to national security.”

• How would you envision these legislative proposals be considered collectively? Would you recommend one piece of legislation to deal with all of these issues in the national security context?

I do not think that it is necessary to have a single piece of legislation. However, I do believe that the Congress, in evaluating each proposal, should consider its
interaction with the other proposals and the possible cumulative effect on national security and the public's right to be informed.

- With regard to state secrets, would you support providing to the congressional intelligence committees regular reports on the assertion of a state secrets privilege, including the classified declarations by the intelligence or other officials in support of those assertions of privilege?

President Obama recently said that the Administration will voluntarily report to Congress regarding when and why the state secrets privilege is invoked, to allow for proper congressional oversight, and if confirmed I would support that effort.

Many of these legislative proposals reflect concern that the Executive Branch does not adequately weigh the public interest when classifying information or when evaluating the interest of the coordinate branches, the courts and Congress, or the public's need for information.

- If you feel that deference should be accorded to Executive Branch determinations relating to the damage to national security from disclosure, how would you recommend addressing the congressional concern about Executive Branch overclassification?

President Obama recently announced a review of Executive Order 12958, specifically including "[e]ffective measures to address the problem of over classification." The Director of National Intelligence is given considerable responsibilities in the area of classification and declassification by the National Security Act and Executive Order 12333 and I would therefore expect that he would play a significant role in this review, as well as the parallel review of procedures relating to Controlled Unclassified Information. If confirmed, I look forward to discussing these issues with the committee.

Cyber security
Mr. Litt, the Obama Administration has undertaken a 60 day review of the Comprehensive National Cybersecurity Initiative. Although you noted in your responses to the Committee’s prehearing questions that our efforts must strictly comply with the Constitution and the law, you did not identify what privacy concerns you thought might be implicated by the government’s involvement in this area.

- What would you identify as the main privacy concerns and civil liberties related to the cybersecurity initiative?

The privacy and civil liberties concerns related to the cybersecurity initiative arise from the vast amount of personal and private data that is stored on electronic networks or transmitted over electronic communications systems. This information is vulnerable to attack by malevolent individuals, but also may be compromised by government action if adequate safeguards are not provided. The challenge will be to provide robust protection for government and private networks and systems that are essential to our national security and our economy, while at the same time protecting individual privacy from unnecessary intrusion.

- Do you see a need for legislative changes to support the cybersecurity initiative?

The review of cybersecurity issues that the President ordered has just been released and I have not yet had an opportunity to review it in detail. If confirmed, however, I expect to be involved in the resolution of any legal issues and will work with the committee on any legislative changes that may be necessary.

**Declassified OLC opinions**

Mr. Litt, on April 16, 2009, the Department of Justice released four opinions that were issued by the Office of Legal Counsel in the last Administration for the CIA. These opinions have been withdrawn by the Department of Justice.

- Do you believe that you are limited in any way in commenting on any of these opinions on account of your representation of a client in private practice?
As I have stated, I do not believe that I can offer an opinion about the legal status of interrogation techniques that may have been employed in the past. While I believe I can comment on some aspects of these opinions there are some areas that I cannot comment upon consistent with my ethical responsibilities.

- To the extent you are able to comment, and focusing for now on the interpretation of the Fifth and Eighth Amendment in the May 30, 2005 opinion, what is your assessment of its legal reasoning and conclusions?

The relevant question under the Fifth and Eighth Amendments is whether, considered in the light of traditional government behavior and contemporary practice, the conduct can be said to "shock the conscience." This can be a complicated analysis requiring examination of the totality of the circumstances, including the nature of and the justification for the conduct. Based upon my review of the May 30, 2005, opinions and on commentary I have read, I believe that the opinions gave insufficient consideration to precedents from the courts and the Executive Branch relating to some of the interrogation techniques analyzed in them.
Declassified OLC opinions

Mr. Preston, in response to prehearing questions about the now declassified OLC opinions, you both stated that as the interrogation practices in question had been stopped pursuant to Executive Order 13491, and the law has changed by virtue of the Hamdan decision, you did not expect to confront the same issues addressed in the August 2002 and May 2005 opinions. While specific practices have been barred, the federal torture statute addressed in those opinions is unchanged, and, of course, the Fifth and Eighth Amendments are unchanged.

- If alternative approaches to interrogation are proposed, would you be required to evaluate them in light of the requirements of the Fifth and Eighth Amendments, and federal statutes?

- If so, from your prior experience in national security law, do you have any views on the general legal analysis in the now declassified opinions about the U.S. Constitution and the federal torture statute?

Guidelines under Executive Order 12333

Mr. Preston, in your response to prehearing questions, you state that, if confirmed, one of your priorities will be to review existing guidelines under Executive Order 12333 and determine what changes may be warranted.

- If confirmed, would you undertake to report to the Committee within three months of the results of your review?
Views on Pending Legislation

Mr. Preston, in your response to a prehearing question on pending legislation involving the state secrets privilege and other matters, you state that the totality of Administration practices should be considered, not just the few cases that have received public attention.

- With regard to state secrets, would you support providing to the congressional intelligence committees regular reports on the assertion of a state secrets privilege, including the classified declarations by the intelligence or other officials in support of those assertions of privilege?

Executive Branch Oversight

Mr. Preston, in your responses to prehearing questions about Executive Branch oversight and the relationship between the CIA General Counsel and other officials of the intelligence community, you emphasize your personal acquaintance with the nominee for the ODNI General Counsel and the new Assistant Attorney General for National Security.

- Please be more specific about your understanding of the offices and procedures involved in Executive Branch oversight, and what you would do to improve Executive Branch oversight.
Questions for the Record from Vice Chairman Bond

Mr. Litt:

USA PATRIOT Act

The next national security legislation on the agenda will address the USA PATRIOT Act sunset provisions of the "lone wolf," roving wiretap, and Section 215 FISA business records court orders. Amazingly, we are still waiting for the Administration's position on these relatively simple provisions.

- How would you advise the President on whether these provisions should be made permanent, extended, or allowed to expire?

To form a judgment on the renewal of these provisions I would need to understand how they have been used and the circumstances in which they might be needed in the future. As much of this information is classified I have not had an opportunity to review it. If confirmed I will do so and look forward to discussing these issues with the committee.

FISA Amendments Act

- The FISA Amendments Act will sunset in 2012. What are your views on the FISA Amendments Act?

As with the three sunsetting provisions of the USA PATRIOT Act, I would need to understand how the FISA Amendments Act has been used and the circumstances that led to its enactment, information that is classified. Oversight of the use of the FISA Amendments Act is one of the responsibilities of the Office of General Counsel and if confirmed I intend to be involved in that process.

Management
• Lawyers managing lawyers is probably one of the most challenging tasks facing a general counsel. Could you please explain your vision for how you intend to manage the ODNI's Office of General Counsel?

I believe that management of a law office requires first of all selection of capable, intelligent lawyers with initiative. While I have not yet had the opportunity to work closely with the lawyers in the Office of General Counsel my impressions so far are favorable. Second, it is important to delegate clearly both authority and responsibility, and to ensure that your expectations are clearly understood by the lawyers with whom you are working. Third, regular communication with the lawyers, and feedback on how well they are meeting your expectations, is essential to keep track of what they are doing; it is my understanding that there are already regular staff meetings which I intend, if confirmed, to continue.

State Secrets

The “State Secrets Protection Act” is currently pending before the Senate Judiciary Committee. In my opinion, the bill in its current form significantly erodes the protections of the judicially-recognized State Secrets privilege.

• What are your thoughts on the utility of preserving the common law approach to the State Secrets privilege?

The President has emphasized that the principle behind the State Secrets privilege is "absolutely necessary to protect national security." Like the President, however, I am concerned that the privilege has been overused. The President has proposed several reforms in the use of the privilege, and if confirmed, I will examine whether those reforms would best be accomplished through Executive Branch action or legislation.
Extraordinary Renditions

- When you served in the Criminal Division and the DAG's Office during the Clinton Administration, did you support the use of extraordinary renditions in terrorism cases?

To the best of my recollection I did not deal with this issue while I was in the Department of Justice.

- Do you believe that extraordinary rendition should remain in the Intelligence Community's tool box?

The term "extraordinary rendition" has been used in several contexts. I believe that there may be cases where it is appropriate to seize someone abroad and return him to the United States without going through formal extradition processes, and that there may also be cases where it is appropriate to seize someone abroad and send him to a third country. Each of these has been called "extraordinary rendition." In no circumstances, however, do I believe it is appropriate to send someone to a country where it is known that he will face torture, and I believe that any rendition to a third country should only be undertaken when there are satisfactory assurances that the individual will be treated properly.

Media Shield

- One of the biggest problems in the Intelligence Community is the seemingly endless leaks of classified information that reveal our sources and methods. Do you believe that those who leak classified information should be prosecuted to the fullest extent of the law?
Leaks of classified information are very serious and in my view if persons who leak classified information can be identified they should be prosecuted.

- Do you think it would be a good idea to create a statutory privilege for journalists (or people who can quickly qualify as journalists by posting a few blogs on the internet) to protect criminals who leak classified information?

The President has expressed his support for responsible media shield legislation, in view of the critical role that the media play in a free and democratic society. I believe that such legislation can and should be crafted to ensure that leaks of classified information can be effectively investigated and prosecuted, and if confirmed I look forward to working with the Congress to ensure that any legislation that is passed does so.

- Wouldn't such a privilege actually encourage even more unauthorized disclosure of classified information?

Again, I believe that legislation creating a statutory privilege for journalists can and should be crafted in a manner to protect intelligence sources and methods and other classified information and that would not encourage unauthorized disclosure of such information.
Questions for the Record from Senator Whitehouse

Mr. Litt:

Please provide your responses to the questions I asked Mr. Preston at the hearing concerning:

- how do you intend to balance the President's desire to look forward with your responsibilities as general counsel to assist in the resolution of very significant unresolved issues of the past pertaining to the treatment of detainees; and

As President Obama has said, it is of critical importance that the Intelligence Community and the nation move forward to address the urgent national security challenges and opportunities facing us, including important decisions as to the appropriate disposition of persons now in our custody or those whom we may detain in the future. I agree, however, that it is important both to be informed about and mindful of past practices in order to ensure that we make the right decisions going forward, and to provide a process that ensures that appropriate actions are taken in regard to these past practices.

- how will you ensure that your principal, the Director of National Intelligence, has access to channels of information and advice on these issues from career officials who were not themselves associated with decisions that led to the torture of detainees?

If confirmed, I will ensure that Director Blair receives expert legal advice and counsel from senior lawyers with no prior involvement in those decisions, and with full access to whatever information is necessary for complete and accurate factual determinations to support that advice and counsel.
Questions for the Record from Senator Levin

Mr. Litt:


Yes.

2. Do you believe that the release of the four OLC opinions has jeopardized national security?

No.

3. Do you believe that waterboarding is torture?

The President and the Attorney General have stated that waterboarding is torture and I have no reason to disagree with that conclusion. Moreover, the President has stated that he has banned waterboarding "once and for all" and Director Blair has stated that it will not occur on his watch. I therefore do not expect to be presented with that legal question, but if confirmed, I can promise that waterboarding will not happen on my watch.

4. Do you believe that there are differences between the interrogation techniques as applied by the Central Intelligence Agency (CIA) and as applied in Survival Evasion Resistance Escape (SERE) training?

While I am not fully familiar either with the manner in which the interrogation techniques were applied by the CIA or with SERE training, materials that I have read indicate that there are differences, for example the fact that SERE training is voluntary and an individual can indicate that he or she wants the technique to stop.
5. General David Petraeus said in a May 10, 2007 letter that “Some may argue that we would be more effective if we sanctioned torture or other expedient methods to obtain information from the enemy. They would be wrong. Beyond the basic fact that such actions are illegal, history shows that they also are frequently neither useful nor necessary. Certainly, extreme physical action can make someone ‘talk’; however, what the individual says may be of questionable value.” Do you agree with General Petraeus?

Yes.

6. What would you do if the Director of National Intelligence (DNI) made a significant public statement that was erroneous or misleading? What would you do if the DNI refused to correct such a statement?

I am confident from my discussions with him that Director Blair is committed to transparency, accuracy and disclosure to the greatest extent possible, consistent with national security. If the Director of National Intelligence made a significant public statement that I believed was erroneous or misleading I would discuss the matter with him to ascertain whether my understanding was correct and, if so, the reason for the Director’s action. If I was not satisfied with the Director’s explanations, and could not convince the Director to correct the statement, I would consider resigning my position if the matter was of sufficient importance.
Questions for the Record from Senator Levin

Mr. Preston:

1. On April 16, 2009, the Department of Justice released four opinions issued by the Office of Legal Counsel (OLC) (dated August 1, 2002, May 30, 2005, and two issued on May 10, 2005). Do you believe that the release of those opinions has jeopardized national security?

2. General David Petraeus said in a May 10, 2007 letter that “Some may argue that we would be more effective if we sanctioned torture or other expedient methods to obtain information from the enemy. They would be wrong. Beyond the basic fact that such actions are illegal, history shows that they also are frequently neither useful nor necessary. Certainly, extreme physical action can make someone ‘talk,’ however, what the individual says may be of questionable value.” Do you agree with General Petraeus?
Questions for the Record from Senator Feingold

Mr. Litt:

Congressional notification

In your responses to Committee questions, you indicated that, under Section 502 of the National Security Act, the DNI could limit briefings to the Chairman and Vice Chairman, using the “Gang of Eight” provision from Section 503 “by analogy.” This is wrong as a matter of statutory interpretation. Please clarify.

Section 502 of the National Security Act provides that the intelligence committees must be kept fully and currently informed “[t]o the extent consistent with due regard for the protection from disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.” My reference to Section 503 was meant only to indicate by analogy the sorts of circumstances under which I thought that a limited briefing might be appropriate under Section 502.

The warrantless wiretapping program (or Terrorist Surveillance Program) was a collection activity covered under Section 502 of the National Security Act. Was the failure to notify the full Committee a violation of that Act?

Because the program you refer to is classified, I am not familiar with it nor with the reasons why the full Committee was not briefed.

What is your understanding of the legal obligation to notify the congressional intelligence committees of covert action and other intelligence activities prior to their implementation?

Section 503 of the National Security Act requires the President to report “before the initiation of [a] covert action” and provides that if the President does not do so he shall fully inform the intelligence committees in a timely fashion and explain why prior notice was not given. Section 502 requires that the intelligence
committees be kept "fully and currently informed" of intelligence activities, including any "significant anticipated intelligence activity," and that any report relating to a significant anticipated intelligence activity should be in writing and contain a concise statement of the facts. As you know, Director Blair has repeatedly emphasized the importance of timely notification to the committees and keeping the committees fully and currently informed. If confirmed, I will fully support the Director's policies.

Warrantless wiretapping

Based on the Bush Administration's 2006 "white paper" and other public sources, do you believe that the warrantless wiretapping program (Terrorist Surveillance Program) was legal under Justice Jackson's steel seizure case test?

Because the program you refer to is classified, I am not sufficiently familiar with it or with the reasons why it was believed to be necessary to offer a view as to whether it was a valid exercise of the President's authorities.

State secrets

The president has committed to "voluntarily reporting to Congress when we have invoked the [state secrets] privilege and why." Will you commit to providing such briefings to Committee members and staff?

Yes.

OLC review

During his confirmation hearing, DNI Blair agreed to send all intelligence programs that pose significant legal questions to the Justice Department's Office of Legal Counsel (OLC), right at the outset. Will you commit to doing this? Will you include the Comprehensive Cybersecurity Initiative?

To the extent that any intelligence issues pose significant legal questions that require the views of the Department of Justice I commit that, if confirmed, I will ensure that they are submitted to the Office of Legal Counsel at the outset. To the
extent that the cybersecurity initiative raises such legal issues, if confirmed I will ensure that they are submitted.

Conflicts of interest

With regard to potential conflicts of interest, you have indicated that you have relied on and will continue to rely on the counsel of the ODNI Designated Agency Ethics Official. That person, however, is an employee of the ODNI Office of the General Counsel (OGC) and thus would be your direct subordinate, should you be confirmed. This raises further questions about objectivity and impartiality. Have you discussed potential conflicts of interest with anyone outside the OGC? Have you had any discussions with the DNI regarding the possibility, should you be confirmed, of designating an ethics official outside the OGC who could provide you counsel and, if so, what was the outcome of those discussions?

The issue you raise is not unique to this particular situation but exists throughout the government. In the Office of the Director of National Intelligence, as in all other federal agencies, the Designated Agency Ethics Officer is subordinate to one or more individuals in the agency to whom he or she gives ethics advice. Thus, for example, the ODNI DAEO is also responsible for giving ethics advice to the Director. The DAEO may call upon experts at the Office of Government Ethics in determining the appropriateness of any potential recusals. I have full confidence in the DAEO’s ability to provide objective and impartial ethics advice and to consult with the office of Government Ethics when she deems it advisable.

You have indicated that the “precise contours” of the scope of your potential conflicts of interest have yet to be determined. This raises the question of when you will voluntarily recuse yourself or seek counsel. You have identified questions of prosecution or investigation, as well as reviews of interrogation techniques that are the “subject of [your] representation” of your clients as posing potential conflicts of interest. While the “subject of [your] representation” of your clients may have been narrow, however, you may be familiar with the broader range of activities conducted by your
clients, and your decisions with regard to these activities going forward could affect not only possible prosecution or investigation, but administrative actions or career advancement. What decisions related to detention, interrogation or rendition might prompt you to recuse yourself or seek counsel? Are there other decisions that might affect the interests of your clients still in the Intelligence Community, such as those related to the relative authorities of the CIA and DNI, the role of contractors, or employee benefits? If so, how will you identify them and what course of action would you take?

As I have told the committee, I will not participate in any decisions relating to the possible prosecution or investigation of my former clients nor any decisions that would affect the outcome of such matters, including decisions about similarly situated individuals or offering an opinion with respect to the legal status of particular interrogation procedures that may have been employed in the past that relate to the subject of my representation. With respect to the types of other decisions you identify, they do not appear to present a conflict, but I will provide the Designated Agency Ethics Official with the names of these former clients to ensure that I do not participate in any matters from which I should be recused.
Questions for the Record from Senator Feingold

Mr. Preston:

Interrogations

Both the Attorney General and the President have indicated that waterboarding is torture. Is this your professional opinion as well?

You indicated during your confirmation hearing that you believe that the four Office of Legal Counsel (OLC) memos recently declassified and withdrawn are "flawed." Please describe the flaws you have identified in those memos.

Renditions

Director Panetta has left the door open for renditions to other countries of individuals in short-term CIA custody. First, what kinds of assurances and follow-up are necessary to satisfy the United States' obligations under the Convention Against Torture? Second, even if those obligations are met, are there legal requirements that the individual be subject to an open legal process, rather than indefinite extrajudicial detention? And, third, is there an obligation to notify the ICRC of such renditions?

OLC review

During his confirmation hearing, DNI Blair agreed to send all intelligence programs that posed significant legal questions to the Office of the Legal Counsel (OLC), right at the outset. Will you commit to doing this? Will you include any resumption of renditions or short-term CIA detentions, or considerations of interrogation policies that diverge from the Army Field Manual?
State secrets

In your response to Committee questions about state secrets legislation, you indicated that Congress should consider the impact on cases currently being litigated. Since then, the President has committed to "voluntarily report to Congress when we have invoked the privilege and why." Will you commit to providing Committee members and staff briefings on cases involving the CIA in which the privilege has been invoked?

Congressional notification

Do you agree that Section 502 of the National Security Act provides no authority to limit briefings to the Chairman and Vice Chairman and that programs other than covert action must always be notified to the full congressional intelligence committees? Was the failure to notify the full committees of the warrantless wiretapping program (the Terrorist Surveillance Program) a violation of that Act?

What is your understanding of the legal obligation to notify the congressional intelligence committees of covert action and other intelligence activities prior to their implementation?

Inspector General

Do you agree that the CIA Inspector General should have full independence to conduct investigations of CIA activities, regardless of whether the General Counsel has concluded that those activities are legal?
RESPONSES OF STEPHEN W. PRESTON

COMMITTEE QUESTIONS FOR THE RECORD

NOMINATIONS OF ROBERT S. LITT AND STEPHEN W. PRESTON

Congressional Notification

Mr. Litt and Mr. Preston, in addition to the responses you have already given concerning congressional notifications, please also respond to the following:

Q: Would you both support, in those circumstances in which the legality of an intelligence activity has been evaluated in a legal opinion of the Department of Justice or of a General Counsel’s Office in the Intelligence Community, providing that opinion to the congressional intelligence committees?

A: I would support providing a legal opinion to the intelligence committees where appropriate in order to keep the committees fully and currently informed of intelligence activities as required by section 502 of the National Security Act of 1947. I do not support an absolute rule – either precluding disclosure of any legal opinion of the Justice Department or of an OGC in the IC to the committees in any instance, or requiring disclosure of all legal opinions of the Justice Department or of an OGC in the IC to the committees in all instances. This is a judgment to be made on a case-by-case basis in light of the particular circumstances and considerations presented.

Q: With respect to the content of limited briefings, what measures would you support to provide for complete records of any such briefings? For example, the establishment of a DNI registry of them? The submission by the DNI or the DCIA of a written statement to the Chairman and Vice Chairman? Non objection to the creation of a congressional record, through the Committee’s cleared reporter or a recording? Other means?

A: I am not sufficiently familiar with the historical practices in conducting and memorializing limited briefings to offer a specific recommendation at this point. I understand that this is a matter of significant concern to the Committee and others, particularly of late, and, if confirmed, I will work
with Director Panetta to address this concern. With respect to briefings by the CIA, I expect that there are means by which the Agency can record the fact and substance of a briefing in a manner that is reliable, accessible as needed, and protective against unauthorized disclosure of classified information.

Q: To determine whether there are matters of continuing interest that were briefed to prior committee leaders but not to the current Committee, would you undertake a review of all limited notifications of the past ten years and provide to the Committee a comprehensive list of them?

A: Again, while I am not conversant with the history of limited notifications, my sense at present is that I would support undertaking an effort of this sort to the extent appropriate in order to keep the committees fully and currently informed of intelligence activities as required by section 502 of the National Security Act of 1947, subject to any direction Director Panetta may provide and coordination with others as appropriate. The focus, I expect, would be on any ongoing intelligence activities that were briefed to prior committee leadership but never disclosed to the full committee.

Q: In the limited cases in which notification to a group smaller than the full committees is provided, what is the statutory basis, if any, for limiting the notification to the Gang of Four (the leaders of the two committees) rather than the full Gang of Eight (thereby including the Leaders)?

A: With respect to intelligence activities other than covert actions, under section 502 of the National Security Act of 1947, the Agency is required to keep the intelligence committees fully and currently informed “to the extent consistent with due regard for the protection from unauthorized disclosure of classified information” that is exceptionally sensitive. The “due regard” clause is a qualification on the obligation, requiring the Agency to inform the committees in a manner consistent with due regard for the protection from unauthorized disclosure of such classified information. I am not sufficiently familiar with the historical practices in providing notification to a group smaller than the full committee to say what circumstances and considerations have led to limiting the notification to the Gang of Four rather than the full Gang of Eight in the past, but any such limitation founded on section 502 must be based on a considered judgment.
that it is necessary under the “due regard” clause. Section 503 of the Act, of course, governs covert actions.

There is an interest on the Committee, reflected in legislative proposals in our authorization bills, in changing the notification provisions in the National Security Act to ensure that the full Committee is informed.

**Q:** Do you think the notification provisions need to be amended?

**A:** At this point, I do not think that the notification provisions need to be amended. Those provisions reflect a delicate balancing of constitutional interests between the Executive branch and the Congress that ought not be unnecessarily disturbed. At the same time, I am keenly aware of the Committee’s concerns with limited briefings, records of same and related issues, and I am committed to working with Director Panetta in addressing these concerns, to the end of improving communication between the Agency and the Committee and, specifically, ensuring that the provisions of section 502 are properly followed. Rather than legislative changes, I favor leadership-level discussions between the Agency and the Committee aimed at developing a common understanding on the issues of concern and on practical procedures to ensure that the full Committee is informed as required by law.

**Q:** Would you work with this Committee in crafting appropriate amendments?

**A:** As noted above, I favor discussions between the Agency and the Committee because I think much can be done to improve notification within the current framework. Subject to any direction Director Panetta may provide and coordination with others as appropriate, I would be happy to work with the Committee on legislative proposals or otherwise to address legal issues that may arise during my tenure.

*The Clients of the National Security Lawyer*

Mr. Preston, during the hearing you were asked about your response to the prehearing questions about the unclassified conclusions of the CIA Inspector General’s report entitled “Procedures Used in Narcotics Airbridge Denial Program in Peru, 1995-2001” and when it might be appropriate to advise clients not to create discoverable documents during civil litigation or while facing the threat of civil litigation. Please provide written responses to these questions:
Q: Does the CIA General Counsel have any responsibilities higher than ensuring that the CIA and all its personnel act in accordance with the law and maintain full and accurate records of their actions?

A: At the most fundamental level, the General Counsel, like every lawyer in the Office of General Counsel, is sworn to uphold and protect the Constitution of the United States. That is an obligation that is not be taken lightly and underlies virtually everything the General Counsel does. Moreover, as I said in my responses to prehearing questions, “[p]erhaps the most important, overarching role of the General Counsel is in ensuring the Agency’s compliance with applicable U.S. law in all of its activities.” By “the Agency,” I mean to include the people who comprise the Agency. And by “compliance with applicable U.S. law in all of its activities,” I would include maintaining full and accurate records where the maintenance of records is required by law or otherwise undertaken.

Q: Does the CIA General Counsel have any role in representing personnel in investigations by the Department of Justice or by the CIA Inspector General?

A: No, the General Counsel represents the Agency, and ultimately the United States and the people of the United States. He takes his direction from the Director. Although the Agency is, in an important sense, the men and women who comprise the Agency, the General Counsel has no role in representing any individual in his or her personal capacity in investigations by the Justice Department or by the CIA IG.

Q: What is the General Counsel’s role in litigation to redress harm to individuals allegedly caused by CIA actions? In your view, is the CIA General Counsel another member of the defense team?

A: In connection with litigation to redress harm to individuals allegedly caused by CIA actions, the General Counsel represents the Agency. He has no role in representing any individual in his or her personal capacity. Depending on the forum and the defendant(s), defense of litigation may be the responsibility of the Department of Justice with support from CIA OGC — in which case the General Counsel functions as the senior representative of the Justice Department’s “client” agency — or the responsibility of CIA OGC — specifically, OGC attorneys reporting to the General Counsel. The General Counsel may bring to a given case a perspective different from
those most actively involved in the defense, but his focus remains on the interests of the Agency.

Confirming General Counsels

Mr. Litt and Mr. Preston, Congress chose to require Senate confirmation for both the DNI and CIA General Counsel positions. Mr. Preston was specifically asked about his understanding of the purpose of the establishment of a confirmed General Counsel of the Central Intelligence Agency.

Q: Mr. Preston, what is your understanding of the purpose of Congress's establishment of a confirmed General Counsel?

A: I regard the requirement of the Senate's advice and consent as an indication of the importance of the position and of the incumbent's role in ensuring the Agency's compliance with applicable U.S. law. In addition, the Committee, in reporting its FY 1997 Intelligence Authorization bill, stated as follows: "The Committee believes that the confirmation process enhances accountability and strengthens the oversight process." S. REP. NO. 258, 104th Cong., 2d Sess. 34 (1998). See also my response to prehearing question 3(a).

Conflicts

Q: Mr. Preston, in addition to informing the Committee about potential conflicts from your private practice, what information can you place on the public record about those conflicts and their resolution?

A: During my tenure as General Counsel, there may arise matters in which a former client of mine is a party or my former law firm represents a party. Pursuant to the terms of my ethics agreement and the Ethics Pledge (Executive Order No. 13490) to which I will be bound if confirmed, I will not participate personally and substantially in any particular matter involving specific parties in which my former law firm is a party or represents a party for a period of two years after my resignation, unless I am first authorized to participate pursuant to 5 C.F.R. 2635.502(d) and paragraph 3 of Executive Order 13490. I also will not participate personally and substantially in any particular matter involving specific parties in which a former client of mine is a party or represents a party for a period of two years after my
resignation, unless I am first authorized to participate pursuant to 5 C.F.R. 2635.502(d) and paragraph 3 of Executive Order 13490.

Upon confirmation and assumption of duties as General Counsel, I will execute a formal recusal in which I will detail the screening arrangement to be used in any particular matter from which I am recused.

In the circumstance that the Director determines my participation is necessary in a matter involving my former firm or a former client from which I am otherwise recused, I will consult with the agency ethics official, who will in turn consult with the Office of Government Ethics, to determine whether an authorization to participate pursuant to 5 C.F.R. 2635.502(d) and a waiver of paragraph 3 of the Executive Order, is appropriate.

**Conflicting legal opinions**

Mr. Litt, in your responses to the Committee’s prehearing questions, you noted that you would work with the CIA General Counsel to ensure that legal issues related to the work of the CIA are reviewed and evaluated. You also indicated that you would work with the general counsels of the various intelligence agencies and with attorneys from the Department of Justice with respect to conflicting legal opinions within the Intelligence Community. You also stated that the DNI General Counsel does not have decisional authority to resolve conflicting legal interpretations in the Intelligence Community.

**Q:** Mr. Preston, will you ensure that the ODNI General Counsel has full awareness of significant legal interpretations by your office?

**A:** The working relationship between ODNI OGC and CIA OGC has been described to me as highly collaborative. In legal matters of Director-level interest or of general interest to the IC, I would expect a free flow of information from CIA OGC to ODNI OGC (and vice versa). In this fashion, the ODNI GC should become fully aware of significant legal interpretations by CIA OGC. Moreover, if I learn of a legal interpretation of which the ODNI GC is not aware that I believe he should be, I will see to it that he is made fully aware of it.
Declassification—IG Reports and OLC Opinions

Mr. Litt, the DNI will likely be involved in recommending whether information about both the Terrorist Surveillance Program and CIA’s detention and interrogation program should be declassified, and will likely seek your counsel on those topics. In your responses to the Committee’s prehearing questions, you noted that the public interest in the disclosure of certain information may outweigh the need to protect it.

Q: Mr. Preston, what are your views on the declassification of the OLC opinions?

A: I support the President’s decision to declassify the four OLC opinions.

Declassified OLC opinions

Mr. Preston, in response to prehearing questions about the now declassified OLC opinions, you both stated that as the interrogation practices in question had been stopped pursuant to Executive Order 13491, and the law has changed by virtue of the Hamdan decision, you did not expect to confront the same issues addressed in the August 2002 and May 2005 opinions. While specific practices have been barred, the federal torture statute addressed in those opinions is unchanged, and, of course, the Fifth and Eighth Amendments are unchanged.

Q: If alternative approaches to interrogation are proposed, would you be required to evaluate them in light of the requirements of the Fifth and Eighth Amendments, and federal statutes?

A: Executive Order 13491 prohibits the use of interrogation techniques not authorized by and listed in the Army Field Manual. The Executive Order also establishes a Special Task Force, chaired by the Attorney General, to determine what if any additional or different techniques necessary to protect national security may be warranted. If alternative approaches to interrogation are proposed, I expect that they would be evaluated under currently applicable U.S. law.

When the U.S. Senate ratified the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment in 1984, it did so with the following reservation: “That the United States considers itself bound by the obligation under article 16 to prevent ‘cruel, inhuman or degrading treatment or punishment,’ only insofar as the term ‘cruel,
inhuman or degrading treatment or punishment’ means the cruel, unusual and inhumane treatment or punishment prohibited by the Fifth, Eighth, and/or Fourteenth Amendments to the Constitution of the United States.” This reservation was carried over to the Detainee Treatment Act of 2005. The Detainee Treatment Act prohibits cruel, inhuman and degrading treatment or punishment of detainees, defined as the cruel, unusual and inhumane conduct prohibited by the 5th, 8th and 14th Amendments. In *Hamdan v. Rumsfeld* (2006), the Supreme Court held that Common Article 3 of the Geneva Conventions applies to terrorist detainees. The Military Commissions Act of 2006 criminalizes cruel or inhuman treatment, listing it with torture and seven other specific activities as among the “grave breaches” of Common Article 3 that constitute a war crime under the War Crimes Act.

The federal torture statute remains applicable, but cruel, inhuman and degrading is generally considered to be a lower threshold/stricter requirement than torture. I would anticipate that any new interrogation techniques to be recommended would have to be evaluated not only under the torture statute and any other federal statutes that applied, but also under the standards of the 5th, 8th, and 14th Amendments per the Detainee Treatment Act, as well as under Common Article 3 of the Geneva Conventions.

**Q:** If so, from your prior experience in national security law, do you have any views on the general legal analysis in the now declassified opinions about the U.S. Constitution and the federal torture statute?

**A:** I have no prior experience with the federal torture statute and am not an expert in the relevant constitutional jurisprudence. However, as noted in my responses to the prehearing questions and in my testimony at the hearing, I believe that the now declassified OLC opinions are flawed. The Department of Justice itself, in the prior Administration, publicly repudiated the reasoning of the unclassified August 1, 2002 opinion and formally withdrew it, later superseding the now declassified August 1, 2002 opinion. The Justice Department has since determined the four opinions to be flawed, having now withdrawn all four. If alternative approaches to interrogation are proposed, I expect that their lawfulness would be assessed by the Department of Justice. In that event, as previously noted, I would become sufficiently familiar with the facts and guiding legal principles to be able to
fully engage with the Justice Department. I would not be bound in any respect by the legal analysis in the now declassified OLC opinions.

Guidelines under Executive Order 12333

Mr. Preston, in your response to prehearing questions, you state that, if confirmed, one of your priorities will be to review existing guidelines under Executive Order 12333 and determine what changes may be warranted.

Q: If confirmed, would you undertake to report to the Committee within three months of the results of your review?

A: I believe this is a fair request, and I will do my best to accommodate the Committee. Because I am not familiar with the existing guidelines or progress towards implementing the current version of Executive Order 12333, I cannot commit to the formal reporting of my views by a certain date or independent of the Agency. That said, I would hope to be in a position to engage with the Committee within a three-month timeframe, subject to any direction Director Panetta may provide and coordination with others as appropriate.

Views on Pending Legislation

Mr. Preston, in your response to a prehearing question on pending legislation involving the state secrets privilege and other matters, you state that the totality of Administration practices should be considered, not just the few cases that have received public attention.

Q: With regard to state secrets, would you support providing to the congressional intelligence committees regular reports on the assertion of a state secrets privilege, including the classified declarations by the intelligence or other officials in support of those assertions of privilege?

A: In remarks delivered at the National Archives on May 21, 2009, the President said, with reference to the State Secrets privilege: "We plan to embrace several principles for reform. We will apply a stricter legal test to material that can be protected under the State Secrets privilege. We will not assert the privilege in court without first following a formal process, including review by a Justice Department committee and the personal approval of the Attorney General. Finally, each year we will voluntarily report to Congress when we have invoked the privilege and why, because
there must be proper oversight of our actions.” I support the President’s decision to change the practices associated with assertion of the State Secrets privilege in these respects, including instituting regular reports to the appropriate oversight committees. Whether to include classified declarations in such reports is, I believe, a judgment to be made on a case-by-case basis in light of the specific circumstances and considerations presented.

Executive Branch Oversight

Mr. Preston, in your responses to prehearing questions about Executive Branch oversight and the relationship between the CIA General Counsel and other officials of the intelligence community, you emphasize your personal acquaintance with the nominee for the ODNI General Counsel and the new Assistant Attorney General for National Security.

Q: Please be more specific about your understanding of the offices and procedures involved in Executive Branch oversight, and what you would do to improve Executive Branch oversight.

A: The DNI has statutory and Executive Order oversight responsibilities for the CIA and the IC generally. Under section 104A(b) of the National Security Act of 1947, the DCIA reports to the DNI “regarding the activities of the [CIA].” In addition, under section 102A(f)(4) of the Act, the DNI has the statutory responsibility to ensure that CIA activities are consistent with the Constitution and laws of the United States. The ODNI GC in turn serves as the senior legal adviser to the DNI. The Assistant Attorney General for National Security (AAG-NSD) has certain responsibilities for oversight and execution with respect to FISA applications, and CT and CI investigations and prosecutions, among other things. Because I am not yet familiar with the procedures and interactions between CIA OGC and ODNI OGC and between CIA OGC and OAAG-NSD — the latter offices having been created since the time of my prior government service — I am unable to describe them with particularity or to make specific recommendations concerning Executive Branch oversight. As previously noted, I believe that highly functional relationships with the ODNI GC and the AAG-NSD are very important. While my prior acquaintance with the ODNI GC nominee and the current AAG-NSD will no doubt help, I am confident that I will have well-functioning relationships with each, no matter who the incumbent is, because I view it as imperative in order for us to get the job done.
QUESTIONS FOR THE RECORD FROM VICE CHAIRMAN BOND

USA PATRIOT Act

The next national security legislation on the agenda will address the USA PATRIOT Act sunset provisions of the “lone wolf,” roving wiretap, and Section 215 FISA business records court orders. Amazingly, we are still waiting for the Administration’s position on these relatively simple provisions.

Q: How would you advise the President on whether these provisions should be made permanent, extended, or allowed to expire?

A: I have not yet been briefed on the details of how the Intelligence Community has used these authorities, so it would be premature for me to advise the President or anyone else on the reauthorization of these provisions at this time. However, among the factors I believe should be considered in determining whether these provisions should be continued are the extent to which the use of these authorities has resulted in intelligence gains for the U.S. and whether the use of these authorities has significantly affected the civil liberty interests of U.S. persons.

FISA Amendments Act

Q: The FISA Amendments Act will sunset in 2012. What are your views on the FISA Amendments Act?

A: I think the FISA Amendments Act, providing procedures for targeting persons outside the United States, was important in supplying a statutory basis and judicial process for certain surveillance previously challenged as unlawful. At this time, I do not have a view on renewal in 2012.

Management

Q: Lawyers managing lawyers is probably one of the most challenging tasks facing a general counsel. Could you please explain your vision for how you intend to manage the CIA’s Office of General Counsel?

A: I have considerable prior experience running the law offices of large federal agencies - the Department of Defense Office of General Counsel and Defense Legal Services Agency, and the Department of the Navy Office of the General Counsel - and managing government attorneys many of whom are collocated with their “client” components within the agency. In my
experience, in addition to basic leadership skills, the following are useful and effective:

Exercising ultimate responsibility for the professional supervision and evaluation of all attorneys providing legal services within the agency;

Maintaining a good supervisory structure and relying on senior staff who are experienced managers;

Providing multiple opportunities for direct communication with rank and file lawyers and support staff; and

Offering rotation and other forms of career enrichment.

State Secrets

The "State Secrets Protection Act" is currently pending before the Senate Judiciary Committee. In my opinion, the bill in its current form significantly erodes the protections of the judicially-recognized State Secrets privilege.

Q: You have served as the Deputy Assistant Attorney General in the Department of Justice's Civil Division. What are your thoughts on the utility of preserving the common law approach to the State Secrets privilege?

A: State Secrets is an important and time-honored, judicially recognized privilege. I would be concerned about any legislative proposal that might impinge upon the President's constitutional responsibility to protect national security information, put in the hands of the courts matters they may not be constitutionally or institutionally competent to decide, and under-protect national security information from disclosure. In remarks delivered at the National Archives on May 21, 2009, the President said, with reference to the State Secrets privilege: "We plan to embrace several principles for reform. We will apply a stricter legal test to material that can be protected under the State Secrets privilege. We will not assert the privilege in court without first following a formal process, including review by a Justice Department committee and the personal approval of the Attorney General. Finally, each year we will voluntarily report to Congress when we have invoked the privilege and why, because there must be proper oversight of our actions." I support the President's decision to change the practices associated with assertion of the State Secrets privilege in these
respects. In my view, these reforms address the issue of “over-use” of the privilege without eroding the protections of or eliminating the common law approach to the privilege.

**Extraordinary Renditions**

**Q:** Do you support the use of extraordinary renditions in terrorism cases? Should the technique remain in the Intelligence Community’s tool box?

**A:** I am not aware of any legal determination that rendition per se is unlawful. Indeed, “extraordinary renditions” are specifically authorized in the U.S. Attorneys Manual as a means to bring individuals overseas into the United States to stand trial. While renditions per se are not unlawful, they must not be used for an unlawful purpose. I am also not aware of any policy decision to prohibit renditions. To the contrary, the practice is one of the things being studied by the Special Task Force chaired by the Attorney General under Executive Order 13491. I look forward to the recommendations of the Special Task Force and, assuming it remains in the “tool box,” am prepared to support lawful rendition in appropriate cases.

**Media Shield**

**Q:** One of the biggest problems in the Intelligence Community is the seemingly endless leaks of classified information that reveal our sources and methods. Do you believe that those who leak classified information should be prosecuted to the fullest extent of the law?

**A:** Yes. At the same time, I understand that there may be considerable difficulty in identifying the source of a leak and that the judgment whether to prosecute the source of a leak may be influenced by the nature and extent of additional disclosure that prosecution would likely entail.

**Q:** Do you think it would be a good idea to create a statutory privilege for journalists (or people who can quickly qualify as journalists by posting a few blogs on the internet) to protect criminals who leak classified information?

**A:** See my response to prehearing question no. 13 for a more detailed discussion. In short, I understand the general concern underlying the question and note three specific concerns:
How to appropriately tailor the definition of the type of journalists to be covered by the legislation, so that only bona fide journalists are included;

How to effectively define the type of information that is subject to the privilege governed by the legislation; and

How to define the role of the courts in assessing whether and how the privilege should be overridden in light of a demonstrated governmental interest, and with deference for the President’s constitutional obligation to protect classified national security information.

Q: Wouldn’t such a privilege actually encourage even more unauthorized disclosure of classified information?

A: I do not know. In my view any such legislation should be framed so as not to encourage leaks, to the extent possible.

QUESTIONS FOR THE RECORD FROM SENATOR LEVIN

Q: On April 16, 2009, the Department of Justice released four opinions issued by the Office of Legal Counsel (OLC) (dated August 1, 2002, May 30, 2005, and two issued on May 10, 2005). Do you believe that the release of those opinions has jeopardized national security?

A: I support the President’s decision to release the four OLC opinions. The potential impact on national security, positive or negative, was among the considerations informing the President’s decision, and the President explained his thinking in this regard in his statement on April 16, 2009.

Q: General David Petraeus said in a May 10, 2007 letter that “Some may argue that we would be more effective if we sanctioned torture or other expedient methods to obtain information from the enemy. They would be wrong. Beyond the basic fact that such actions are illegal, history shows that they also are frequently neither useful nor necessary. Certainly, extreme physical action can make someone ‘talk;’ however, what the individual says may be of questionable value.” Do you agree with General Petraeus?

A: Yes, I agree with General Petraeus that sanctioning torture would be wrong. I also agree that torture is illegal. As the effectiveness of interrogation techniques is an area in which I have no training or experience, I am not in a position to assess the utility of extreme physical
action as a means of obtaining valuable information or its necessity as opposed to alternative techniques. But I have no basis for disagreeing with General Petraeus in this regard. Finally, I should reiterate that, by order of the President, the Agency does not and will not engage in torture. If I am confirmed, it certainly will not during my tenure as General Counsel.

QUESTIONS FOR THE RECORD FROM SENATOR FEINGOLD

Interrogations

Q. Both the Attorney General and the President have indicated that waterboarding is torture. Is this your professional opinion as well?

A: As I testified at the hearing, I support the President's and the Attorney General's conclusion that waterboarding is torture, and the President's decision that the United States will not engage in the practice going forward. I have not made an independent legal judgment with respect to past conduct under the federal torture statute, but I have no reason to disagree with the conclusion reached by the President and the Attorney General.

Q: You indicated during your confirmation hearing that you believe that the four Office of Legal Counsel (OLC) memos recently declassified and withdrawn are "flawed." Please describe the flaws you have identified in those memos.

A: Some flaws apparent to me after reviewing the four OLC opinions (without examining applicable precedents or otherwise conducting any legal research) are as follows:

One problem with all of the memos is the assumption that the Geneva Conventions, including Common Article 3 and its proscriptions against inhumane treatment, violence to life or person (including cruel treatment) and outrages upon personal dignity (including humiliating and degrading treatment), were inapplicable. The error of this assumption was conclusively established by the Supreme Court in Hamdan v. Rumsfeld.

In the unclassified August 1, 2002 memo (portions of which the previously classified August 1, 2002 memo referred to):

The discussion of the President's Commander-in-Chief power and the defenses of necessity and self-defense in the unclassified August 1, 2002
memo overreaches and betrays a result-orientation not typical in OLC jurisprudence.

The proposition that physical pain amounting to torture must be equivalent in intensity to the pain accompanying serious physical injury such as organ failure, impairment of bodily function or even death was erroneous and later recognized as such.

The proposition that there is no concept of physical suffering amounting to torture apart from physical pain was erroneous and later recognized as such.

The proposition, in the May 10, 2005 Techniques memo (and unclassified December 30, 2004 memo), that physical suffering amounting to torture must be extreme in intensity and significantly protracted in duration or persistent over time – as opposed to extreme in intensity and difficult to endure, as for physical pain – was dubious and insufficiently supported.

The May 10, 2005 Combined Techniques memo is flawed at least to the extent that the analysis of individual techniques is flawed. In addition, in its effort to show that the whole is nothing more than the sum of its parts, the memo loses sight of the possibility that the repeated application of certain techniques in the course of an interrogation could supply the “protracted” or “persistent” physical suffering (or “prolonged” or “extended” mental harm) found absent in any single application.

The May 30, 2005 memo rejects U.S. military doctrine as reflected in the Army Field Manual as a possible measure of what would “shock the conscience” on the basis that a policy premised on the applicability of the Geneva Conventions does not constitute controlling evidence of executive tradition and contemporary practice with respect to untraditional armed conflict where those treaties do not apply. The Court in Hamdan, of course, overturned this erroneous premise.

Renditions

Q: Director Panetta has left the door open for renditions to other countries of individuals in short-term CIA custody. First, what kinds of assurances and follow-up are necessary to satisfy the United States’ obligations under the Convention Against Torture? Second, even if those obligations are met, are there legal requirements that the
individual be subject to an open legal process, rather than indefinite extrajudicial detention? And, third, is there an obligation to notify the ICRC of such renditions?

**A:** Article 3 of the Convention Against Torture forbids transferring a person to another country "where there are substantial grounds for believing that he would be in danger of being subjected to torture." When the Senate ratified the Convention Against Torture, it did so with an understanding that the phrase, "where there are substantial grounds for believing that he would be in danger of being subjected to torture" means "if it is more likely than not that he would be tortured." Therefore, the United States may not render a person to another country where it is more likely than not that the person would be tortured. In determining whether it is more likely than not a person would be torture, the United States is charged by Article 3 of the Convention to "take into account all relevant considerations including, where applicable, the existence in the State concerned of a consistent pattern of gross, flagrant or mass violations of human rights."

I am not aware of a legal requirement that a country must agree to submit a person to an open legal process as a condition of rendering a person there. The United States could make a policy choice to seek such a commitment and, if it did so, I would ensure that policy choice was respected.

Finally, Executive Order 13491 would require the CIA to notify the ICRC of CIA detainees "consistent with Department of Defense regulations and policies."

**OLC Review**

**Q:** During his confirmation hearing, DNI Blair agreed to send all intelligence programs that posed significant legal questions to the Office of the Legal Counsel (OLC), right at the outset. Will you commit to doing this? Will you include any resumption of renditions or short-term CIA detentions, or considerations of interrogation policies that diverge from the Army Field Manual?

**A:** In matters of exceptional significance or sensitivity, particularly with issues potentially affecting multiple agencies, where there may be conflicting views within the Executive branch, or with issues outside the Agency's expertise, I believe that it is entirely appropriate and wise to seek learned and authoritative legal guidance from the Department of Justice. Although I
do not think it is necessary to submit all intelligence programs or all significant legal questions to OLC for review/analysis, I have every intention to make liberal use of OLC when confronted with legal issues arising from intelligence programs. Moreover, with respect to the particular activities cited – resumption of renditions and divergence from the Army Field Manual – it is difficult to imagine either occurring without substantial consultation with OLC. I certainly would want the benefit of OLC’s legal analysis.

State Secrets

Q: In your response to Committee questions about state secrets legislation, you indicated that Congress should consider the impact on cases currently being litigated. Since then, the President has committed to “voluntarily report to Congress when we have invoked the privilege and why.” Will you commit to providing Committee members and staff briefings on cases involving the CIA in which the privilege has been invoked?

A: In remarks delivered at the National Archives on May 21, 2009, the President said, with reference to the State Secrets privilege: “We plan to embrace several principles for reform. We will apply a stricter legal test to material that can be protected under the State Secrets privilege. We will not assert the privilege in court without first following a formal process, including review by a Justice Department committee and the personal approval of the Attorney General. Finally, each year we will voluntarily report to Congress when we have invoked the privilege and why, because there must be proper oversight of our actions.” I support the President’s decision to change the practices associated with assertion of the State Secrets privilege in these respects, including instituting regular reports to the intelligence committees. While I am not sure what form such reporting will take, I would favor reporting to the entire membership of the Committee as the norm (with staff as appropriate).

Congressional Notification

Q: Do you agree that Section 502 of the National Security Act provides no authority to limit briefings to the Chairman and Vice Chairman and that programs other than covert action must always be notified to the full congressional intelligence committees? Was the failure to notify the
Full committees of the warrantless wiretapping program (the Terrorist Surveillance Program) a violation of that Act?

A: With respect to intelligence activities other than covert actions, under section 502 of the National Security Act of 1947, the Agency is required to keep the intelligence committees fully and currently informed "to the extent consistent with due regard for the protection from unauthorized disclosure of classified information" that is exceptionally sensitive. The "due regard" clause is a qualification on the obligation, requiring the Agency to inform the committees in a manner consistent with due regard for the protection from unauthorized disclosure of such classified information. Thus the law requires the complete and timely provision of information to the intelligence committees and admits of exception only in extraordinary circumstances. In my view, the norm should be to provide information to the entire membership of the committees.

Q: What is your understanding of the legal obligation to notify the congressional intelligence committees of covert action and other intelligence activities prior to their implementation?

A: With respect to covert actions, section 503 of the National Security Act of 1947 requires that a finding be reported to the intelligence committees "before the initiation of the covert activity," but also provides for notice "in a timely fashion" where prior notice is not given. With respect to intelligence activities other than covert actions, section 502 of the Act does not include the same "before the initiation" language, but does include "significant anticipated intelligence activities" among the intelligence activities to be reported, subject to the "due regard" clause. In my view, the norm should be to provide information prior to implementation.

Inspector General

Q: Do you agree that the CIA Inspector General should have full independence to conduct investigations of CIA activities, regardless of whether the General Counsel has concluded that those activities are legal?

A: I believe that the Inspector General should have full independence to conduct investigations of CIA activities within the scope of the Inspector General's statutory authority. By law, pursuant to section 20 of the CIA Act of 1949, the General Counsel of the Central Intelligence Agency is the chief
legal officer of the Agency. As such, the General Counsel is the final 
authority for the Agency in matters of law and legal policy, and his legal 
opinions are controlling within the Agency. Rather than the General 
Counsel unilaterally declaring lawful activities already under investigation 
or the Inspector General initiating an investigation of activities previously 
determined to have been lawful, this strikes me as a prime example of where 
the two ought to work together to ensure that the considered opinions of the 
former and the full independence of the latter are both respected.
COUNTERINTELLIGENCE

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE
Annex A
Intelligence Community and Private Sector Measures to Counter Economic Espionage and Manage Collection in Cyberspace ................................................................. A-1

Annex B
West and East Accuse China and Russia of Economic Espionage .................................................. B-1

List of Text Boxes
Non-Cyber Methods of Economic Espionage ...................................................................................... 2
The Cost of Economic Espionage to One Company .......................................................................... 3
A Possible Proxy Measure of the Costs of Economic Espionage to the United States ...................... 4

List of Charts
Recent Insider Thefts of Corporate Trade Secrets with a Link to China ........................................... 4
Russian Leaders Link Intelligence Operations and Economic Interests ............................................ 6
Projected Growth in Number of IT Devices Connected to Networks and the Internet, 2003-2020 ...... 7
Rising Prices Increase Value of Commodity Information to Foreign Collectors ............................. 9
Executive Summary

Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation’s prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.

US Technologies and Trade Secrets at Risk in Cyberspace

Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods.

Economic espionage incurs costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimate of the monetary value of these costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees. Moreover, victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits.

Pervasive Threat from Adversaries and Partners

Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.

- Chinese actors are the world’s most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.
- Russia’s intelligence services are conducting a range of activities to collect economic information and technology from US targets.
- Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment.

- Over the next several years, the proliferation of portable devices that connect to the Internet and other networks will continue to create new opportunities for malicious actors to conduct espionage. The trend in both commercial and government organizations toward the pooling of information processing and storage will present even greater challenges to preserving the security and integrity of sensitive information.
• The US workforce will experience a cultural shift that places greater value on access to information and less emphasis on privacy or data protection. At the same time, deepening globalization of economic activities will make national boundaries less of a deterrent to economic espionage than ever.

We judge that the governments of China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace.

The relative threat to sensitive US economic information and technologies from a number of countries may change in response to international economic and political developments. One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of aggressive cyber and other espionage against US technologies and economic information.

Although foreign collectors will remain interested in all aspects of US economic activity and technology, we judge that the greatest interest may be in the following areas:

• Information and communications technology (ICT), which forms the backbone of nearly every other technology.
• Business information that pertains to supplies of scarce natural resources or that provides foreign actors an edge in negotiations with US businesses or the US Government.
• Military technologies, particularly marine systems, unmanned aerial vehicles (UAVs), and other aerospace/aeronautic technologies.
• Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy and healthcare/pharmaceuticals.

Cyberspace provides relatively small-scale actors an opportunity to become players in economic espionage. Under-resourced governments or corporations could build relationships with hackers to develop customized malware or remote-access exploits to steal sensitive US economic or technology information, just as certain PIS have already done.

• Similarly, political or social activists may use the tools of economic espionage against US companies, agencies, or other entities, with disgruntled insiders leaking information about corporate trade secrets or critical US technology to "hacktivist" groups like WikiLeaks.
Scope Note

This assessment is submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, as amended, which requires that the President biennially submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the 14th Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008 and draws primarily on data from 2009-2011.

New Focus and Additional Resources Used for This Year's Report

This report differs from previous editions in three important ways. The first and most significant is the focus. This report gives special attention to foreign collectors' exploitation of cyberspace, while not excluding other established tactics and methods used in foreign economic collection and industrial espionage. This reflects the fact that nearly all business records, research results, and other sensitive economic or technology-related information now exist primarily in digital form. Cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with little risk, whether via remote exploitation of victims’ computer networks, downloads of data to external media devices, or e-mail messages transmitting sensitive information.

The second difference from prior reports is that, in addition to researching the large body of intelligence reporting and analysis on economic espionage produced by the Intelligence Community, the Department of Defense (DoD), and other US Government agencies, the drafters of this report consulted new sources of government information.

Third, the Office of the National Counterintelligence Executive (ONCIX) mobilized significant resources from outside the IC during the course of this study. This included outreach to the private sector and, in particular, sponsorship of a conference in November 2010 on cyber-enabled economic espionage at which 26 US Government agencies and 21 private-sector organizations were represented. ONCIX also contracted with outside experts to conduct studies of the academic literature on the cost of economic espionage and the role of the cyber “underground economy.”

Definitions of Key Terms

For the purposes of this report, key terms were defined according to both legal and analytic criteria.

The legal criteria derive from the language in the Economic Espionage Act (EEA) of 1996 (18 USC §§ 1831-1839). The EEA is concerned in particular with economic espionage and foreign activities to acquire US trade secrets. In this context, trade secrets are all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if the owner (the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to acquire these secrets include the following criminal offenses:

• Economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1831).
• **Industrial espionage**, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).

The following definitions reflect the experience of IC cyber, counterintelligence, and economic analysts:

• **Cyberspace** is the interdependent network of information technology (IT) infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

• **Sensitive** is defined as information or technology (a) that has been classified or controlled by a US Government organization or restricted in a proprietary manner by a US corporation or other institution, or (b) that has or may reasonably be expected to have military, intelligence, or other uses with implications for US national security, or (c) that may enhance the economic competitiveness of US firms in global markets.

**Contributors**

ONCIX compiled this report using inputs and reporting from many US Government agencies and departments, including the Air Force Office of Special Investigations (AFOSI), Army Counterintelligence Center (ACIC), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Health and Human Services (HHS), Department of State (DoS), Federal Bureau of Investigation (FBI), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Naval Criminal Investigative Service (NCIS).
Foreign Spies Stealing US Economic Secrets in Cyberspace

US Technologies and Trade Secrets at Risk in Cyberspace

The pace of foreign economic collection and industrial espionage activities against major US corporations and US Government agencies is accelerating. Firms, corporations, and private individuals increased their efforts in 2009-2011 to steal proprietary technologies, which cost millions of dollars to develop and represent tens or hundreds of millions of dollars in potential profits. The computer networks of a broad array of US Government agencies, private companies, universities, and other institutions—all holding large volumes of sensitive economic information—were targeted by cyber espionage; much of this activity appears to have originated in China.

Increasingly, economic collection and industrial espionage occur in cyberspace, reflecting dramatic technological, economic, and social changes that have taken place in recent years in the ways that economic, scientific, and other sensitive information is created, used, and stored. Today, nearly all business records, research results, and other sensitive economic data are digitized and accessible on networks worldwide. Cyber collection can take many forms, including: simple visits to a US company’s website for the collection of openly available information; a corporate insider’s downloading of proprietary information onto a thumb drive at the behest of a foreign rival; or intrusions launched by Firms or other actors against the computer networks of a private company, federal agency, or an individual.

The Appeal of Collecting in Cyberspace

Cyberspace is a unique complement to the espionage environment because it provides foreign collectors with relative anonymity, facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.

Security and attribution. Collectors operating in a cyber environment can collect economic information with less risk of detection. This is particularly true for remote computer network exploitation (CNE). Foreign collectors take advantage of the fact that it is difficult to detect and to attribute responsibility for these operations.

There is increasing similarity between the tools, tactics, and techniques used by various actors, which reduces the reliability of using these factors to identify those responsible for computer network intrusions.

- The proliferation of malicious software (malware) presents opportunities for intelligence services and other actors to launch operations with limited resources and without developing unique tools that can be associated with them.
- Hacker websites are prevalent across the internet, and tool sharing is common, causing intrusions by unrelated actors to exhibit similar technical characteristics.
- Firms and other foreign entities have used independent hackers at times to augment their capabilities and act as proxies for intrusions, thereby providing plausible deniability.
- Many actors route operations through computers in third countries or physically operate from third countries to obscure the origin of their activity.

Another factor adding to the challenge of attribution is the diverging perspectives of the actual targets of economic espionage in cyberspace.

- At a conference sponsored by ONCIX in November 2010, US private industry representatives said they saw little difference between cybercrime—for example, identity theft or the misappropriation of intellectual property such as the counterfeiting of commercial video or audio recordings—and the collection of economic or technology information by intelligence services or other foreign entities. Private sector organizations are often less concerned with attribution and focus instead on damage control and prevention; moreover, few companies have the ability to identify cyber intruders.
• US Government law enforcement and intelligence agencies, on the other hand, seek to establish attribution as part of their mission to counter EIS and other clandestine information collectors. They, unlike companies, also have the intelligence collection authorities and capabilities needed to break multiple layers of cover and to establish attribution where possible.

Cyberspace also offers greater security to the perpetrator in cases involving insiders. Although audits or similar cyber security measures may flag illicit information downloads from a corporate network, a malicious actor can quickly and safely transfer a data set once it is copied. A physical meeting is unnecessary between the corrupted insider and the persons or organizations the information is being collected for, reducing the risk of detection.

**Faster and cheaper.** Cyberspace makes possible the near instantaneous transfer of enormous quantities of economic and other information. Until fairly recently, economic espionage often required that insiders pass large volumes of documents to their handlers in physical form—a lengthy process of collection, collation, transportation, and exploitation.

• Dongfan Chung was an engineer with Rockwell and Boeing who worked on the B-1 bomber, space shuttle, and other projects and was sentenced in early 2010 to 15 years in prison for economic espionage on behalf of the Chinese aviation industry. At the time of his arrest, 250,000 pages of sensitive documents were found in his house. This is suggestive of the volume of information Chung could have passed to his handlers between 1979 and 2006. The logistics of handling the physical volume of these documents—which would fill nearly four 4-drawer filing cabinets—would have required considerable attention from Chung and his handlers. With current technology, all the data in the documents hidden in Chung’s house would fit onto one inexpensive CD.  

**Extra-territoriality.** In addition to the problem of attribution, it often is difficult to establish the geographic location of an act of economic espionage that takes place in cyberspace. Uncertainty about the physical location of the act provides cover for the perpetrators and complicates efforts by US Government law enforcement or intelligence agencies to respond.

**Non-Cyber Methods of Economic Espionage**

Although this assessment focuses on the use of cyber tools and the cyber environment in foreign efforts to collect sensitive US economic information and technologies, a variety of other methods also remain in use.

**Requests for Information (RFI).** Foreign collectors make unsolicited direct and indirect requests for information via personal contacts, telephone, e-mail, fax, and other forms of communication and often seek classified, sensitive, or export-controlled information.

**Solicitation or Marketing of Services.** Foreign companies seek entrée into US firms and other targeted institutions by pursuing business relationships that provide access to sensitive or classified information, technologies, or projects.

**Conferences, Conventions, and Trade Shows.** These public venues offer opportunities for foreign adversaries to gain access to US information and experts in dual-use and sensitive technologies.

**Official Foreign Visitors and Exploitation of Joint Research.** Foreign government organizations, including intelligence services, use official visits to US Government and cleared defense contractor facilities, as well as joint research projects between foreign and US entities, to target and collect information.

**Foreign Targeting of US Visitors Overseas.** Whether traveling for business or personal reasons, US travelers overseas—businesspeople, US Government employees, and contractors—are routinely targeted by foreign collectors, especially if they are assessed

---

*Chung was prosecuted only for possession of these documents with the intent to benefit the People’s Republic of China (PRC) and acting as an unregistered foreign agent for China. He was not charged with communication of this information to the PRC or any other foreign entity.

*On average, one page of typed text holds 2 kilobytes (KB) of data; thus, 250,000 pages x 2 KB/page = 500,000 KB, or 488 megabytes (MB). A data CD with a capacity of 700 MB retails for $0.75, and a flashdrive with a capacity of 4 gigabytes costs about $13.00.*
as having access to some sensitive information. Some US allies engage in this practice, as do less friendly powers such as Russia and China. Targeting takes many forms: exploitation of electronic media and devices, surreptitious entry into hotel rooms, aggressive surveillance, and attempts to set up sexual or romantic entanglements.

**Open Source Information.** Foreign collectors are aware that much US economic and technological information is available in professional journals, social networking and other public websites, and the media.

**Large but Uncertain Costs**

Losses of sensitive economic information and technologies to foreign entities represent significant costs to US national security. The illicit transfer of technology with military applications to a hostile state such as Iran or North Korea could endanger the lives of US and allied military personnel. The collection of confidential US Government economic information—whether by a potential adversary or a current ally—could undercut US ability to develop and enact policies in areas ranging from climate change negotiations to reform of financial market regulations. The theft of trade secrets from US companies by foreign economic rivals undermines the corporate sector’s ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security.

Data on the effects of the theft of trade secrets and other sensitive information are incomplete, however, according to an ONCIX-sponsored survey of academic literature on the costs of economic espionage.

- Many victims of economic espionage are unaware of the crime until years after loss of the information.
- Even when a company knows its sensitive information has been stolen by an insider or that its computer networks have been penetrated, it may choose not to report the event to the FBI or other law enforcement agencies. No legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company’s reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.

- A company also may not want to publicly accuse a corporate rival or foreign government of stealing its secrets from fear of offending potential customers or business partners.

- Finally, it is inherently difficult to assign an economic value to some types of information that are subject to theft. It would, for example, be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a US company and foreign counterparts.

**The Cost of Economic Espionage to One Company**

Data exist in some specific cases on the damage that economic espionage or theft of trade secrets has inflicted on individual companies. For example, an employee of Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new job in China, according to press reports. This theft represented about one-eighth of Valspar’s reported profits in 2009, the year the employee was arrested.

Even in those cases where a company recognizes it has been victimized by economic espionage and reports the incident, calculation of losses is challenging and can produce ambiguous results. Different methods can be used that yield divergent estimates, which adds to the difficulty of meaningfully comparing cases or aggregating estimated losses.

- An executive from a major industrial company told ONCIX representatives in late 2010 that his company has used historical costs—tallying salaries, supplies, utilities, and similar direct expenses—to estimate losses from cases of attempted theft of its trade secrets. This method has the advantage of using known and objective
data, but it underestimates the extent of losses in many cases because it does not capture the effect of lost intellectual property on future sales and profits.

- Harm is calculated in US civil court cases involving the theft of trade secrets by measuring the "lost profits" or "reasonable royalty" that a company is unable to earn because of the theft. Although this method requires subjective assumptions about market share, profitability, and similar factors, it does offer a more complete calculation of the cost than relying strictly on historical accounting data.

- Estimates from academic literature on the losses from economic espionage range so widely as to be meaningless—from $2 billion to $400 billion or more a year—reflecting the scarcity of data and the variety of methods used to calculate losses.

A Possible Proxy Measure of the Costs of Economic Espionage to the United States

New ideas are often a company’s or an agency’s most valuable information and are usually of greatest interest to foreign collectors. Corporate and government spending on research and development (R&D) is one measure of the cost of developing new ideas, and hence is an indicator of the value of the information that is most vulnerable to economic espionage. R&D spending has been tracked by the National Science Foundation (NSF) since 1953. For 2008, the most recent year available, the NSF calculated that US industry, the Federal Government, universities, and other nonprofit organizations expended $398 billion on R&D, or 2.8 percent of the US Gross Domestic Product.

Pervasive Threat from Intelligence Adversaries and Partners

Many states view economic espionage as an essential tool in achieving national security and economic prosperity. Their economic espionage programs combine collection of open source information, HUMINT, signals intelligence (SIGINT), and cyber operations—to include computer network intrusions and exploitation of insider access to corporate and proprietary networks—to develop information that could give these states a competitive edge over the United States and other rivals.

- China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology.

- Other countries with closer ties to the United States have conducted CNE and other forms of intelligence collection to obtain US economic and technology data, often taking advantage of the access they enjoy as allies or partners to collect sensitive military data and information on other programs.

Recent Insider Thefts of Corporate Trade Secrets with a Link to China

David Yen Lee...chemist with Valspar Corporation...between late 2008 and early 2009 used access to internal computer network to download about 160 secret formulas for paints and coatings to his own storage media...intended to take this proprietary information to a new job with Nippon Paint in Shanghai, China...arrested March 2009...pleaded guilty to one count of theft of trade secrets; sentenced in December 2010 to 15 months in prison.

Meng Hong...DuPont Corporation research chemist...in mid-2009 downloaded proprietary information on organic light-emitting diodes (OLED) to personal e-mail account and thumb drive...intended to transfer this information to Peking University, where he had accepted a faculty position; sought Chinese Government funding to commercialize OLED research...arrested October 2009...pleaded guilty to one count of theft of trade secrets; sentenced in October 2010 to 14 months in prison.

Yu Xiang Dong (aka Mike Yu)...product engineer with Ford Motor Company who in December 2006 accepted a job at Ford’s China branch...copied approximately 4,000 Ford documents onto an external hard drive to help obtain a job with a Chinese automotive company...arrested in October 2009...pleaded guilty to two counts of theft of trade secrets; sentenced in April 2011 to 70 months in prison.
China: Persistent Collector

Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector.

China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail. Of the seven cases that were adjudicated under the Economic Espionage Act—both Title 18 USC § 1831 and § 1832—in Fiscal Year 2010, six involved a link to China.

US corporations and cyber security specialists also have reported an onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China, which private sector specialists call "advanced persistent threats." Some of these reports have alleged a Chinese corporate or government sponsor of the activity, but the IC has not been able to attribute many of these private sector data breaches to a state sponsor. Attribution is especially difficult when the event occurs weeks or months before the victims request IC or law enforcement help.

- In a February 2011 study, McAfee attributed an intrusion set they labeled "Night Dragon" to an IP address located in China and indicated the intruders had exfiltrated data from the computer systems of global oil, energy, and petrochemical companies. Starting in November 2009, employees of targeted companies were subjected to social engineering, spear-phishing e-mails, and network exploitation. The goal of the intrusions was to obtain information on sensitive competitive proprietary operations and on financing of oil and gas field bids and operations.

- In January 2010, VeriSign iDefense identified the Chinese Government as the sponsor of intrusions into Google's networks. Google subsequently made accusations that its source code had been taken—a charge that Beijing continues to deny.

- Mandiant reported in 2010 that information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm. Mandiant's report indicated that the US manufacturing company lost sensitive data on a weekly basis and that this may have helped the Chinese firm attain a better negotiating and pricing position.

- Participants at an ONCIX conference in November 2010 from a range of US private sector industries reported that client lists, merger and acquisition data, company information on pricing, and financial data were being extracted from company networks—especially those doing business with China.

Russia: Extensive, Sophisticated Operations

Motivated by Russia's high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward US and other Western interests at the expense of Russia, Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security.

- For example, the IC Russian Foreign Intelligence Service (SVR) "illegals" arrested in June 2010 were tasked to collect economic and technology information, highlighting the importance of these issues to Moscow.¹

¹An "illegal" is an officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he or she is connected or with the government operating that intelligence organization.
Russian Leaders Link Intelligence Operations and Economic Interests

The SVR “must be able to swiftly and adequately evaluate changes in the international economic situation, understand the consequences for the domestic economy and...more actively protect the economic interests of our companies abroad.”

—Vladimir Putin, President, Russian Federation, October 2007

“Intelligence...aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology.”

—Mikhail Fradkov, Director, SVR, December 2010

Source: Russian press reports.

US Partners: Leveraging Access

Certain allies and other countries that enjoy broad access to US Government agencies and the private sector conduct economic espionage to acquire sensitive US information and technologies. Some of these states have advanced cyber capabilities.

Outlook

Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will remain at high levels and continue to threaten US economic security. The nature of these attempts will be shaped by the accelerating evolution of cyberspace, policy choices made by the economic and political rivals of the United States, and broad economic and technological developments.

Near Certainties

Evolving cyber environment. Over the next three to five years, we expect that four broad factors will accelerate the rate of change in information technology and communications technology in ways that are likely to disrupt security procedures and provide new openings for collection of sensitive US economic and technology information. These were identified in studies conducted by Cisco Systems and discussed at the ONCIx conference in November 2010. At the same time, the growing complexity and density of cyberspace will provide more cover for remote cyber intruders and make it even harder than today to establish attribution for these incidents.

The first factor is a technological shift. According to a Cisco Systems study, the number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. This will cause a proliferation in the number of operating systems and endpoints that malicious actors such as foreign intelligence services or corrupt insiders can exploit to obtain sensitive information. Meanwhile, the underlying hardware and software of information systems will become more complex.

• Marketing and revenue imperatives will continue to lead IT product vendors to release products with less than exhaustive testing, which will also create opportunities for remote exploitation.

An economic shift will change the way that corporations, government agencies, and other organizations share storage, computing, network, and application resources. The move to a “cloud computing” paradigm—which is much cheaper for companies than hosting computer services in-
Projected Growth in Number of IT Devices Connected to Networks and the Internet, 2003-2020

<table>
<thead>
<tr>
<th>Millions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>2003</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>60,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: CISCO Systems

house—will mean that employees will be able to work and access data anywhere and at any time, and not just while they are at the office, laboratory, or factory. Although cloud computing offers some security advantages, such as robust backup in the event of a systems disruption, the movement of data among multiple locations will increase the opportunities for theft or manipulation by malicious actors.

The cultural shift involves the rise in the US workforce of different expectations regarding work, privacy, and collaboration. Workers will tend to draw few distinctions between their home and work lives, and they will expect free access to any information they want—whether personal or professional—from any location.

- Current technology already enables many US workers to conduct business from remote locations and on-the-go at any time of day. This alteration relies on the ability of workers to connect to one another and their companies through the Internet—increasing their flexibility and corporate productivity but potentially increasing the risk of theft.

Finally, a geopolitical shift will continue the globalization of economic activities and knowledge creation. National boundaries will deter economic espionage less than ever as more business is conducted from wherever workers can access the Internet. The globalization of the supply chain for new—and increasingly interconnected—IT products will offer more opportunities for malicious actors to compromise the integrity and security of these devices.

Little change in principal threats. The IC anticipates that China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace. Both will almost certainly continue to deploy significant resources and a wide array of tactics to acquire this information from US sources, motivated by the desire to achieve economic, strategic, and military parity with the United States.

China will continue to be driven by its longstanding policy of “catching up fast and surpassing” Western powers. An emblematic program in this drive is Project 863, which provides funding and guidance for efforts to clandestinely acquire US technology and sensitive economic information. The project
was launched in 1986 to enhance China’s economic competitiveness and narrow the science and technology gap between China and the West in areas such as nanotechnology, computers, and biotechnology.

- The growing interrelationships between Chinese and US companies—such as the employment of Chinese-national technical experts at US facilities and the off-shoring of US production and R&D to facilities in China—will offer Chinese Government agencies and businesses increasing opportunities to collect sensitive US economic information.
- Chinese actors will continue conducting CNE against US targets.

Two trends may increase the threat from Russian collection against US economic information and technology over the next several years.

- The many Russian immigrants with advanced technical skills who work for leading US companies may be increasingly targeted for recruitment by the Russian intelligence services.
- Russia’s increasing economic integration with the West is likely to lead to a greater number of Russian companies affiliated with the intelligence services—often through their employment of ostensibly retired intelligence officers—doing business in the United States.

Technologies likely to be of greatest interest. Although all aspects of US economic activity and technology are of potential interest to foreign intelligence collectors, we judge that the highest interest may be in the following areas.

Information and communications technology (ICT). ICT is a sector likely to remain one of the highest priorities of foreign collectors. The computerization of manufacturing and the push for connectedness mean that ICT forms the backbone of nearly every other technology used in both civilian and military applications.

- Beijing’s Project 863, for example, lists the development of “key technologies for the construction of China’s information infrastructure” as the first of four priorities.

Military technologies. We expect foreign entities will continue efforts to collect information on the full array of US military technologies in use or under development. Two areas are likely to be of particular interest:

- Marine systems. China’s desire to jump-start development of a blue-water navy—to project power in the Taiwan Strait and defend maritime trade routes—will drive efforts to obtain sensitive US marine systems technologies.
- Aerospace/aeronautics. The air supremacy demonstrated by US military operations in recent decades will remain a driver of foreign efforts to collect US aerospace and aeronautics technologies. The greatest interest may be in UAVs because of their recent successful use for both intelligence gathering and kinetic operations in Afghanistan, Iraq, and elsewhere.

Civilian and dual-use technologies. We expect that foreign collection on US civilian and dual-use technologies will follow overall patterns of investment and trade. The following sectors—which are expected to experience surges in investment and are priorities for China—may be targeted more aggressively.

- Clean technologies. Energy-generating technologies that produce reduced carbon dioxide and other emissions will be the fastest growing investment sectors in nine of 11 countries recently surveyed by a US consulting company—a survey that included China, France, and India.
- Advanced materials and manufacturing techniques. One focus of China’s 863 program is achieving mastery of key new materials and advanced manufacturing technologies to boost industrial competitiveness, particularly in the aviation and high-speed rail sectors. Russia and Iran have aggressive programs for developing and collecting on one specific area of advanced materials development: nanotechnology.
Rising Prices Increase Value of Commodity Information to Foreign Collectors (Index, 2002=100)

*2011 values as of April.
* Source: International Monetary Fund, World Economic Outlook Database.

- **Healthcare, pharmaceuticals, and related technologies.** Healthcare services and medical devices/equipment will be two of the five fastest growing international investment sectors, according to a US consulting firm. The massive R&D costs for new products in these sectors—up to $1 billion for a single drug—the possibility of earning monopoly profits from a popular new pharmaceutical, and the growing need for medical care by aging populations in China, Russia, and elsewhere are likely to drive interest in collecting valuable US healthcare, pharmaceutical, and related information.

- **Agricultural technology.** Surging prices for food—which have increased by 70 percent since 2002, according to the food price index published by the International Monetary Fund (IMF)—and for other agricultural products may increase the value of and interest in collecting on US technologies related to crop production, such as genetic engineering, improved seeds, and fertilizer.

---

Business information. As with technologies, we assess that nearly all categories of sensitive US economic information will be targeted by foreign entities, but the following sectors may be of greatest interest:

- **Energy and other natural resources.** Surging prices for energy and industrial commodities—which have increased by 210 percent and 96 percent, respectively, since 2002 according to IMF indices—may make US company information on these resources priority targets for intelligence services and other collectors.

- As noted earlier, cyber intrusions originating in China, but not necessarily attributed to the Chinese Government, since at least 2009 have targeted sensitive operational and project-financing information of US and other international oil, energy, and petrochemical companies, according to reports published by McAfee.

---

The IMF's Food Price Index is a weighted index that includes the spot prices of cereal grains, vegetable oils and protein meals, meat, seafood, sugar, bananas, and oranges.

The Fuel (energy) index published by the IMF is a weighted index that includes the spot prices of crude oil, natural gas, and coal. The Industrial Inputs Index is a weighted index that includes the spot price of agricultural raw materials (timber, fibers, rubber and hides) and non-precious metals (such as copper, aluminum, and iron ore).
Business deals. Some foreign companies—sometimes helped by their home countries’ intelligence services—will collect sensitive information from US economic actors that are negotiating contracts with or competing against them.

Macroeconomic information. In the wake of the global financial crisis of 2008-2009 and related volatility in the values of currencies and commodities, sensitive macroeconomic information held by the US private sector and government agencies is likely to remain a prime collection target for both intelligence services and foreign corporations. Chinese and Russian intelligence collectors may pursue, for example, non-public data on topics such as interest rate policy to support their policymakers’ efforts to advance the role of their currencies and displace the dollar in international trade and finance. Such information also could help boost the performance of sovereign wealth funds controlled by governments like China’s, whose China Investment Corporation managed more than $300 billion in investments as of late 2010.¹

Possible Game Changers

Any of a range of less-likely developments over the next several years could increase the threat from economic espionage against US interests.

Emergence of new state threats. The relative threat to sensitive US economic information and technologies from different countries is likely to evolve as a function of international economic and political developments.

One or more fast-growing regional powers may judge that changes in its economic and political interests merit the risk of an aggressive program of espionage against US technologies and sensitive economic information.

Growing role of non-state and non-corporate actors. The migration of most business and technology development activities to cyberspace is making it easier for actors without the resources of a nation-state or a large corporation to become players in economic espionage. Such new actors may act as surrogates or contractors for intelligence services or major companies, or they could conduct espionage against sensitive US economic information and technology in pursuit of their own objectives.

Hackers for hire. Some intelligence services with less-developed cyber programs already use relationships with nominally independent hackers to augment their capabilities to target political and military information or to carry out operations against regime enemies. For example, the Iranian Cyber Army, a hacker group with links to the Iranian Government, has used social engineering techniques to obtain control over Internet domains and disrupt the political opposition, according to research conducted under an ONCIX contract.

No evidence of involvement by independent hackers in economic espionage has been found in intelligence or academic reporting to date, in large part due to the absence of a profitable market for the resale of stolen information. This “cyber underground” could, however, become a fruitful recruiting ground for the tools and talents needed to support economic espionage. Following the model used by some intelligence services in exploiting the cyber environment for political or military espionage, a foreign government or corporation could build relationships with hackers for the development of customized malware or remote access exploits for the exfiltration of sensitive US economic or technology information.

Hacktivists. Political or social activists also may use the tools of economic espionage against US companies, agencies, or other entities. The self-styled whistleblowing group WikiLeaks has already published computer files provided by corporate insiders indicating allegedly illegal or unethical behavior at a Swiss bank, a Netherlands-based commodities company, and an international pharmaceutical trade association. LulzSec—another hacktivist group—has exfiltrated data from several businesses that it posted for public viewing on its website.

¹A sovereign wealth fund is a government investment fund, funded by foreign currency reserves but managed separately from official currency reserves. In other words, it is a pool of money that a government invests for profit.
Corporate trade secrets or information about critical US technology may be at similar risk of disclosure to activist groups by disgruntled insiders.

- Antipoverty activists, for instance, could seek to publish the details of a new medicine under development by a US pharmaceutical company, with the goal of ending the firm's "monopoly" profits and making the product more widely available.
- Antiwar groups could disclose information about a new weapons system in the hope of dissuading the United States from deploying it.
Annex A

Intelligence Community and Private Sector Measures to Counter Economic Espionage and Manage Collection in Cyberspace

The IC is working closely with all segments of the public and private sectors to try to counter espionage activities that target our sensitive economic data and technology. We cannot expect to stop entirely or prevent hostile activity to collect US public and private sector information, but we can work to minimize the activity and mitigate its effects.

Intelligence Community Responses

The IC and especially counterintelligence (CI) officers have already taken a number of steps to improve collaboration, collection, and analysis across the CI, economics, and cyber disciplines.

Improved collaboration. Over the past few years, the IC has established multiple organizations and working groups to better understand the cyber espionage threat. These have contributed to a better understanding of the use of cyber in economic espionage.

- The National Cyber Counterintelligence Working Group established in 2011 is composed of 16 IC and other federal agencies and is creating a coordinated response to the cyber intelligence threat.
- The FBI is leading the National Cyber Investigative Joint Task Force, which brings together multiple agencies to collaborate on intrusions into US systems.

CI officers are considering an expansion of collaboration to include enhanced information sharing with Department of Justice attorneys. CI officers could introduce questions for attorneys to pose to offenders during the investigation process. They might also look at ways to tie plea bargains and sentencing decisions to suspects’ willingness to cooperate with the CI Community during damage assessments.

Improved analysis and collection. The IC has made great strides over the past few years in understanding the cyber espionage threat to US Government systems, but our knowledge of cyber-enabled economic espionage threats to the US private sector remains limited.

Defense Model Shows Limits to Mandatory Reporting Requirements

DoD’s partnership with cleared defense contractors (CDCs) highlights difficulties in establishing an effective framework to improve the IC’s understanding of foreign cyber threats and promote threat awareness in industry. The defense industrial base conducts $400 billion in business with the Pentagon each year and maintains a growing repository of government information and intellectual property on unclassified networks. CDCs are required to file reports of suspicious contacts indicative of foreign threats—including cyber—to their personnel, information, and technologies.

- Despite stringent reporting requirements for CDCs, DSS reports that only 10 percent of CDCs actually provide any sort of reporting in a given year.
- Another shortcoming of the defense model is that contractors do not always report theft of intellectual property unless it relates specifically to Pentagon contracts, according to outreach discussions with corporate officers.
- Corporate security officers also have noted that US Government reporting procedures are often cumbersome and redundant, with military services and agencies such as DSS and the FBI often seeking the same information but in different formats.

Operations. CI professionals are adapting how they detect, deter, and disrupt collection activity in cyberspace because of the challenges in detecting the traditional indicators of collection activity—spotting, assessing, and recruiting.
It is imperative that we improve our ability to attribute technical and human activity in the cyber environment so that we can improve our understanding of the threat and our ability to generate a greater number of offensive CI responses.

Training and awareness. Expanding our national education and awareness campaign aimed at individuals and corporations is an essential defensive strategy for countering threats from cyber-enabled economic collection and espionage. We are building on current outreach initiatives that the FBI and ONCIX have already initiated.

- IC outreach to all US Government agencies, state and local governments, academia, nongovernmental organizations, industry associations, and companies is critical for promoting threat awareness, as well as for a better understanding of nongovernmental perspectives. Partners outside the IC are becoming aware of the wide range of potentially sensitive information in their possession and the extent of foreign efforts to acquire it.

- Outreach efforts include awareness and mitigation strategies for insider threat issues. The unique access of insiders to information technology systems and organizational processes makes this the most dangerous approach to cyber economic collection and espionage, as insiders can act alone to guide CNE or to download sensitive data to portable media.

ONCIX already engages in dialogue with ASIS International—an industry association for security professionals—and the Department of State's Overseas Security Advisory Council on the challenges facing both the public and private sectors with regard to cyber-enabled economic collection and espionage.

Finally, IC outreach efforts to the private sector on economic espionage need to fully engage corporate and other partners in order to be credible. We can facilitate partnerships to share best practices, threat updates and analysis, and data on intrusions. One company security officer has suggested that the IC must speak to industry in language geared to the private sector's needs and experience and emphasize, for example, that the protection of trade secrets is critical to corporate profitability and growth.

As a follow-up to the public/private sector Workshop on Cyber-Enabled Economic Espionage held in 2010, ONCIX should consider sponsoring another conference with Department of Justice and private sector stakeholders on lessons learned regarding successful convictions under Section 1831 of the Economic Espionage Act.

Corporate Responses

The private sector already has a fiduciary duty to account for corporate risk and the bottom-line effects of data breaches, economic espionage, and loss or degradation of services. A key responsibility of chief executive officers and boards of directors is to ensure that the protection of trade secrets and computer networks is an integral part of all corporate decisions and processes and that all managers—not just security and information systems officials—have a stake in the outcome.** Viewing network security and data protection as a business matter that has a significant impact on profitability will lead to more effective risk management and ensure that adequate resources are allocated to address cyber threats to companies.

- Only 5 percent of corporate chief financial officers are involved in network security matters, and just 13 percent of companies have a cross-functional cyber risk team that bridges the technical, financial, and other elements of a company, according to a 2010 study.

Judicial Mandate for Boards of Directors To Secure Corporate Information

Delaware's Court of Chancery ruled in the 1996 Caremark case that a director's good faith duty includes a duty to attempt to ensure that a corporate

---

*Legal and human resources officers are two sets of key stakeholders given the role that corporate insiders have historically played in contributing to economic espionage and the theft of trade secrets.*
information and reporting system exists and that failure to do so may render a director liable for losses caused by the illegal conduct of employees. The Delaware Supreme Court clarified this language in the 2006 Stone v. Ritter case—deciding that directors may be liable for the damages resulting from legal violations committed by the employees of a corporation, if directors fail to implement a reporting system or controls or fail to monitor such systems.

Companies that successfully manage the economic espionage threat realize and convey to their employees that threats to corporate data extend beyond company firewalls to include other locations where company data is moved or stored. These include cloud sites, home computers, laptops, portable electronic devices, portable data assistants, and social networking sites.

- A survey of 200 information technology and security professionals in February 2011 revealed that 65 percent do not know what files and data leave their enterprise.
- According to a March 2011 press report, 57 percent of employees save work files to external devices on a weekly basis.
- E-mail systems are often less protected than databases yet contain vast quantities of stored data. E-mail remains one of the quickest and easiest ways for individuals to collaborate—and for intruders to enter a company’s network and steal data.

Cyber threats to company information are compounded when employees access data through portable devices or network connections while traveling overseas. Many FIS co-opt hotel staffs to allow access to portable devices left unattended in rooms. It is also much easier for FIS to monitor and exploit network connections within their own borders.

- Foreign collectors engage in virtual methods to collect sensitive corporate data and take advantage of victims’ reluctance to report digital penetrations and low awareness of foreign targeting, according to legal academic research.

Corporate security officers have told ONCIX that US Government reporting procedures on economic espionage and cyber intrusions are often cumbersome and redundant. Agencies such as DSS and the FBI often seek the same information but in different formats.
Best Practices in Data Protection Strategies and Due Diligence for Corporations

Information Strategy

- Develop a "transparency strategy" that determines how closed or open the company needs to be based on the services provided.

Insider Threat Programs and Awareness

- Institute security training and awareness campaigns; convey threats to company information accessed through portable devices and when traveling abroad.

- Establish an insider threat program that consists of information technology-enabled threat detection, foreign travel and contact notifications, personnel security and evaluation, insider threat awareness and training, and reporting and analysis.

- Conduct background checks that vet users before providing them company information.

- Implement non-disclosure agreements with employees and business partners.

- Establish employee exit procedures; most employees who steal intellectual property commit the theft within one month of resignation.

Effective Data Management

- Get a handle on company data—not just in databases but also in e-mail messages, on individual computers, and as data objects in web portals; categorize and classify the data, and choose the most appropriate set of controls and markings for each class of data; identify which data should be kept and for how long. Understand that it is impossible to protect everything.

- Establish compartmentalized access programs to protect unique trade secrets and proprietary information; centralize intellectual property data—which will make for better security and facilitate information sharing.

- Restrict distribution of sensitive data; establish a shared data infrastructure to reduce the quantity of data held by the organization and discourage unnecessary printing and reproduction.

Network Security, Auditing, and Monitoring

- Conduct real-time monitoring/auditing of the networks; maintain thorough records of who is accessing servers, and modifying, copying, deleting, or downloading files.

- Install software tools—content management, data loss prevention, network forensics—on individual computer workstations to protect files.
- Encrypt data on servers and password-protect company information.

- Incorporate multi-factor authentication measures—biometrics, PINs, and passwords combined with knowledge-based questions—to help verify users of information and computer systems.

- Create a formal corporate policy for mobility—develop measures for centrally controlling and monitoring which devices can be attached to corporate networks and systems and what data can be downloaded, uploaded, and stored on them.

- Formalize a social media policy for the company and implement strategies for minimizing data loss from on-line social networking.

**Contingency Planning**

- Establish a continuity of operations plan—back up data and systems; create disaster recovery plans; and plan for data breach contingencies.

- Conduct regular penetration testing of company infrastructure as well as of third-party shared service provider systems.

- Establish document creation, retention, and destruction policies.

**Resources for Help**

- Contact ONCIX or the FBI for assistance in developing effective data protection strategies. If a data breach is suspected, contact the FBI or other law enforcement/organizations for help in identifying and neutralizing the threat.
Annex B

West and East Accuse China and Russia of Economic Espionage

Other advanced industrial countries principally blame China and Russia for economic espionage that results in large but uncertain monetary costs and job losses. They perceive that China and Russia continue to use traditional human and technical collection methods—particularly against small- and medium-sized businesses—to gather economic information and technologies that save them research and development (R&D) resources and provide entrepreneurial and marketing advantage for their corporate sectors.

- Germany’s Federal Office for the Protection of the Constitution (BfV) estimates that German companies lose $28 billion-$71 billion and 30,000-70,000 jobs per year from foreign economic espionage. Approximately 70 percent of all cases involve insiders.
- South Korea says that the costs from foreign economic espionage in 2008 were $82 billion, up from $26 billion in 2004. The South Koreans report that 60 percent of victims are small- and medium-sized businesses and that half of all economic espionage comes from China.⁴
- Japan’s Ministry of Economy, Trade, and Industry conducted a survey of 625 manufacturing firms in late 2007 and found that more than 35 percent of those responding reported some form of technology loss. More than 60 percent of those leaks involved China.

France’s Renault Affair Highlights Tendency to Blame China

Brood French concerns with Chinese economic espionage formed the background of the hasty—and subsequently retracted—accusations by corporate and political leaders in January 2011 that three top executives with the Renault automobile company had taken bribes from China in exchange for divulging technology.

- An investigation by the French internal security service revealed that the accusations against China lacked substance and may have stemmed from a corrupt corporate security officer’s attempts to generate investigative work for a friend’s consulting business.

Past Chinese economic espionage against the French automotive industry—including the parts manufacturer Valeo—probably made the French willing to give credence to any accusation of similar malfeasance against China.

Countries acknowledge the growing use of cyber tools for foreign economic collection and espionage and often note difficulties in understanding losses associated with these cyber collection methods. A 2010 survey of 200 industry executives from the power, oil, gas, and water sectors in 12 Western countries, China, and Russia indicates that 85 percent of respondents experienced network intrusions and that government-sponsored sabotage and espionage was the most often cited cyber threat.

- A 2010 Canadian Government report claimed that 86 percent of large Canadian corporations had been hit and that cyber espionage against the private sector had doubled in two years, according to a press report.
- The German BfV offers no reliable figures on the number of cases and amount of damage caused by cyber-enabled economic espionage, adding that their intelligence services are “gropping in the dark.” The German Government has noted the use of CNE tools and removable media devices, claiming that $99 million are spent annually for IT security.
- UK officials note that the cost of an information security incident averages between $16,000 and $32,000 for a small company and between

⁴We have no information on the methodologies that the Germans and South Koreans used to calculate their losses.
$1.6 million and $3.2 million for firms with more than 500 employees. The United Kingdom estimates that attacks on computer systems, including industrial espionage and theft of company trade secrets, cost the private sector $34 billion annually, of which more than 40 percent represents theft of intellectual property such as designs, formulas, and company secrets.

- Germany and South Korea judge that China, in particular, increasingly uses cyber tools to steal trade secrets and achieve plausible deniability, according to press reporting.\(^b\)

- Unidentified CNE operators have accessed more than 150 computers at France’s Finance Ministry since late 2010, exfiltrating and redirecting documents relating to the French G-20 presidency to Chinese sites, according to a press report.

- The British Security Service’s Center for the Protection of National Infrastructure warned hundreds of UK business leaders in 2010 of Chinese economic espionage practices, including giving gifts of cameras and memory sticks equipped with cyber implants at trade fairs and exhibitions. This followed similar notification sent to 300 UK business leaders in 2007 warning them of a coordinated cyber espionage campaign against the British economy.

- German officials also noted that business travelers’ laptops are often stolen during trips to China. The Germans in 2009 highlighted an insider case in which a Chinese citizen downloaded highly sensitive product data from the unidentified German company where he worked to 170 CDs.

- The Director-General of the British Security Service publicly stated that Russia, as well as China, is targeting the UK’s financial system.

- A Russian automotive company bribed executives at South Korea’s GM-Daewoo Auto and Technology to pass thousands of computer files on car engine and component designs in 2009, according to a press report.

- A German insider was convicted of economic espionage in 2008 for passing helicopter technology to the Russian SVR in exchange for $10,000. The insider communicated with his Russian handler through anonymous e-mail addresses.

**Countries Suspect Each Other of Committing Economic Espionage**

Allies often suspect each other of economic espionage—underlining how countries can be partners in traditional security matters yet competitors in business and trade. Foreign corporate leaders may make accusations that are not publicly endorsed by their governments.

- According to a 2010 press report, the Germans view France and the United States as the primary perpetrators of economic espionage "among friends."

- France’s Central Directorate for Domestic Intelligence has called China and the United States the leading “hackers” of French businesses, according to a 2011 press report.

---

\(^{b}\) We lack insight on the processes that the Germans and South Koreans used to attribute cyber activities to China.
Some countries exercise various legislative, intelligence, and diplomatic options to respond to the threat of cyber-enabled economic collection and espionage.

- France and South Korea have proposed new legislation or changes to existing laws to help mitigate the effects of economic espionage. France also is considering a public economic intelligence policy and a classification system for business information.
- France, the United Kingdom, and Australia have issued strategies and revamped bureaucracies to better align resources against cyber and economic espionage threats. France created a 12-person Economic Intelligence Office in 2009 to coordinate French corporate intelligence efforts. The United Kingdom established an Office of Cyber Security to coordinate Whitehall policy under a senior official and a Cyber Security Operations Centre within the Government Communications Headquarters (GCHQ) SIGINT unit. Australia created a cyber espionage branch within its Security Intelligence Organization in 2010.
- The United Kingdom is mobilizing its intelligence services to gather intelligence on potential threats and for operations against economic collection and espionage in cyberspace, according to press reports.

German Espionage Legislation Has Limited Results

Germany's Federal Prosecutor General initiated 31 preliminary proceedings on espionage in 2007, resulting in just one arrest and one conviction. German authorities note that espionage cases are often hindered by diplomatic immunity protections and by attribution issues from operating abroad through cyberspace.

Nearly all countries realize that public and private partnerships are crucial to managing the effects of cyber-enabled economic collection and espionage. The United Kingdom notes that 80 percent of its critical national infrastructure is owned and operated by the private sector, German authorities would like more corporate feedback and say that most enterprises either do not know when they are victims of cyber espionage or do not want to publicly admit their weaknesses. Most countries engage in some form of corporate outreach.

- The French intelligence services offer regular threat briefings to private companies, according to press reports.
- German authorities regularly exchange information with corporate security officers through a private/public working group that includes Daimler AG, Volkswagen, Porsche, Bayer, the German post office, and the railroad industry.

Corporate Leaders Speak Out on Chinese Espionage

Some foreign corporate executives have singled out Chinese espionage as a threat to their companies.

- British entrepreneur James Dyson—inventor of the bagless vacuum cleaner—warned in 2011 that Chinese students were stealing technological and scientific secrets from UK universities, according to a press report. He noted that Chinese students were also planting software bugs that would relay information to China even after their departure from the universities.
- The CEO of an Australian mining firm said that worries over Chinese and other corporate espionage drove him to adopt a more transparent quarterly pricing mechanism for commodities such as iron ore. He claimed that selling products at market-clearing prices visible to all would minimize the impact of differential information that one party may hold, according to a press article.
Sed Quis Custodiet Ipsos Custodes:
The CIA’s Office of General Counsel?

A. John Radsan*

After 9/11, two officials at the Central Intelligence Agency (CIA) made decisions that led to major news. In 2002, one CIA official asked the Justice Department’s Office of Legal Counsel (OLC) to clarify how aggressive CIA interrogators could be in questioning al Qaeda operatives held overseas.¹ This request led to the August 2002 memorandum, later leaked, in which John Yoo argued that an interrogator crosses the line into torture only by inflicting pain on a par with organ failure.² Yoo further suggested that interrogators would have many defenses, justifications, and excuses if they faced possible criminal charges.³ One commentator described the advice as that of a “mob lawyer to a mafia don on how to skirt the law and stay out of prison.”⁴ To cool the debate about torture, the Bush administration retracted the memorandum and replaced it with another.⁵

The second decision was made in 2003, when another CIA official asked the Justice Department to investigate possible misconduct in the disclosure to the media of the identity of a CIA employee. The employee was Valerie Plame, a covert CIA analyst and the wife of Ambassador Joseph Wilson.

---

* Associate Professor of Law, William Mitchell College of Law. The author was a Justice Department prosecutor from 1991 until 1997, and Assistant General Counsel at the Central Intelligence Agency from 2002 until 2004. He thanks Paul Kelbaugh, a veteran CIA lawyer in the Directorate of Operations, for thoughtful comments on an early draft, and Erin Sindberg Porter and Ryan Check for outstanding research assistance. The manuscript of this article was submitted for prepublication review by the CIA, but the views expressed here are solely those of the author.


3. Id.


Plame was mentioned in a Robert Novak article. Her husband had been selected by the Bush administration to determine whether there was any truth to allegations that Iraq had obtained "yellow cake" from Niger for use in building nuclear bombs. After a visit to Niger, Ambassador Wilson wrote an op-ed piece that criticized the Bush administration's case for war against Iraq. When the Justice Department acted on the CIA's request, Attorney General Ashcroft stepped aside from the investigation. Patrick Fitzgerald, United States Attorney for the Northern District of Illinois, was then appointed as special counsel to investigate the "outing" of Plame as possible retaliation against Wilson. As a result of the Fitzgerald investigation, in 2005 a federal grand jury in Washington, D.C. indicted I. Lewis "Scooter" Libby, the Vice President's chief of staff, for perjury, false statements, and obstruction of justice. Libby was subsequently convicted of making false statements and obstructing justice. For a while, even Karl Rove, President Bush's chief political adviser, was in the investigation's cross-hairs.

The CIA officials involved in the two decisions to request assistance from the Justice Department were, respectively, John Rizzo and Scott Muller. Rizzo was Acting General Counsel of the CIA at the time of the first decision. Muller was General Counsel, Rizzo his deputy, when the second decision was made.

Muller, a political appointee, resigned from the CIA in 2004, leaving career lawyer Rizzo at the helm. The reason Muller offered for his departure was a desire to remodel a home in Connecticut with his brother. Lawyers at the CIA, accustomed to elaborate cover stories, thought that story sounded too much like the generic explanations that so often accompany firings in the nation's capital.

6. Robert Novak, The Mission to Niger, CHI. SUN-TIMES, July 14, 2003, at 31. For many CIA officers, the outing conjured up nightmares from the 1970s, when disgruntled former CIA case officer Philip Agee and others embarked on a hateful crusade to reveal CIA identities.
9. See Lichtblau, supra note 8.
13. Muller has joined the New York office of Davis Polk & Wardwell.
is a skill that takes time to develop. More important for the CIA’s General Counsel, sizing up the staff is not as easy as it might be at, say, the Department of Education. Many of the people she deals with, particularly the case officers in the DO, are masters of deception.

Before the position of Director of National Intelligence (DNI) was created at the end of 2004, the DCI wore two different hats. First, he was head of the CIA. Second, he was head of the intelligence community, including the tactical intelligence arms of the military services, the National Security Agency, the Department of State, and the FBI. To advise the DCI about “community management,” OGC used to have a special group of lawyers who helped the DCI keep his two hats straight. Since the DCI no longer wears the second hat, which is now worn by the DNI, OGC’s special group on “community issues” has been assigned to other duties. Now the DNI has the coordinating role and a legal staff to advise him. Now the DNI will try, where the DCI failed, to convince various intelligence agencies to work together in the common cause.

Even with the 2004 legislative changes, the CIA did not lose positions in OGC. Moreover, the DNI has his own General Counsel, creating new jobs for lawyers on intelligence matters. Some OGC lawyers may transfer on their own to assignments at the Office of the DNI or in other intelligence agencies. Their security clearances give them a significant advantage over applicants from outside the intelligence community.\[42\]

III. DIFFERING VIEWS ON THE ROLE OF OGC

Not much has been written in law reviews about the CIA’s General Counsel, yet a number of scholars, General Counsels, and commentators have expressed their views about this office and its holder in other fora.\[43\]


\[43\] Ryan Check, who assisted with this article, canvassed a range of views about the lawyers’ function in the intelligence community. See Ryan M. Check, Who’s the Boss?: The “Public Interest vs. Agency Interest” Balancing Act of Intelligence Agency General Counsels (Apr. 23, 2007) (unpublished manuscript on file with the author). Mr. Check posed three questions about the role of intelligence community general counsels: (1) Should GCs lean toward protecting the agency’s interest or the public interest? (2) To what extent should GCs alter their counsel based purely on the interests of those outside the agency? (3) Can the GC perform an internal oversight function while retaining the confidence of agency management? Experts who responded to these questions included John A. Rizzo (CIA Acting General Counsel), Jeffrey Breinholt (Deputy Chief, Counterterrorism Section, National Security Division, U.S. DOJ), Marion “Spike” Bowman (former Counsel, National Security Law, FBI), Dana Priest (National Security Correspondent, Washington Post), Paul Kelbaugh (former Chief Legal Counsel, CIA Latin America), Richard Cinquegrana (former Special Counsel, CIA DDI), Robert Delahunt (former Deputy General Counsel, White House Office of Homeland Security), Robert F. Turner (former Counsel to President’s Intelligence Oversight Board), David Koplow (former Deputy GC, International Affairs, U.S. DOD), Dr. Dieter Pieluck (former
A. Scholars

In the wake of the Iran-Contra scandal in the 1980s, several articles were written about the oversight of intelligence activities, but none of them focused on CIA’s OGC. More recently, Kenneth J. Levit, a former Special Counsel to the DCI, wrote an article that discusses CIA lawyers’ role in aggressive interrogations since September 11. Because Levit had more experience in the Director’s suite than in the OGC trenches, however, he tends to concentrate on the work of CIA lawyers in the two-part approval process for covert action—approval first within the Agency and second at the National Security Council. He displays great confidence in that process: “If the President ordered actions that would violate the law, lawyers throughout the Agency, as well as those at the National Security Council, would be aware of it, and they would have the chance to voice strong concerns or to object outright.” To Levit, this opportunity to object is significant. Implicit in his thesis is the conviction that 1991 amendments to the National Security Act, which provide more oversight for CIA activities, preclude Agency actions that are kept completely secret from the American public, from Congress, and even from parts of the CIA not directly involved. Moreover, in a footnote he observes, “The CIA’s culture of fidelity to the law would at least guarantee that such problematic claims [the President directing the CIA to engage in torture] would be thoroughly vetted.” In Levit’s mind, the CIA is not a rogue elephant.

Not everyone shares Levit’s faith. This article takes a position somewhere between the believers and the atheists, and seeks to provide enough facts and hunches for agnostics to decide for themselves.

B. The Lawyers Speak About Themselves

Self-reflections are often significant. But CIA lawyers, current and former, are shy about going on the record with examinations of their activities. Those who do go on the record tend to be General Counsels and former General Counsels. So far, we have had Senate hearings on the nominations of two General Counsel candidates, Scott Muller and John Rizzo. Each of the hearings provides clues about the role the nominee sees for himself, as well as

---

44. In 1994 Dorian Greene wrote a fine article that generally discusses lawyers in the intelligence community, but it does not dig into the specific dilemmas that lawyers face at CIA. See Greene, supra note 24.
46. Id. at 352.
47. Id. at 352 n.42.
the role the Senators see. These congressional-executive exchanges, in open
sessions of the intelligence committees, also provide important insights into
the OGC's role in internal oversight.

Robert McNamara was the first nominee for CIA General Counsel who
required Senate confirmation. Before his nomination on October 21, 1997,
McNamara had extensive experience as a government lawyer, having served
for sixteen years in the Treasury Department. He was also Deputy Director
for Enforcement at the Commodity Futures Trading Commission, General
Counsel at the Peace Corps, an Assistant United States Attorney, and a staffer
on the Senate Watergate Committee. 48 McNamara's selection did not create
any controversy. The Senate Select Committee on Intelligence, not interested
in probing the nominee's views about the proper role of the General Counsel,
chose not to hold a hearing. They voted in his favor on November 7, 1997.49
The full Senate confirmed McNamara the next day.50 He turned out to be a
competent but distant leader, more inclined toward oversight than facilitation.
Career lawyers found amusing the frequency with which McNamara reminded
them that he was the first Senate-confirmed General Counsel.

The next nominee was Scott Muller. Before his nomination to be CIA
General Counsel, Muller, like McNamara, had experience as an Assistant
United States Attorney, and he had served on the Watergate prosecution team.
For many years after that, he had worked as a criminal defense lawyer,
focused on white-collar issues and regulatory enforcement matters.

Muller had a one-day hearing on October 9, 2002.51 Muller's friend,
Senator Kit Bond from Missouri, introduced him to the Senate Committee.
The only other Senators who attended were Bob Graham from Florida and Jay
Rockefeller from West Virginia, both Democrats. As Muller admitted to the
Senate Committee, he did not have much experience in the intelligence
community. But that was a minor concern to the Senators. Senator Graham
had a greater concern:

I know from my work on this Committee for the past 10 years that
lawyers at CIA sometimes have displayed a risk aversion in the advice
they give their clients, particularly some of the lawyers
assigned to the posts in the Directorate of Operations. Unfortunately,

48. See Office of the Press Secretary, President Clinton Names Robert McNamara, Jr.
as General Counsel at the Central Intelligence Agency (Oct. 21, 1997), available at http://fas.
49. Presidential Nomination of Robert M. McNamara, Jr., to be General Counsel of the
Central Intelligence Agency, PN792-105, Rec'd by the 105th Congress, Oct. 31, 1997,
available at http://thomas.loc.gov/home/nomis.html (search "Robert M. McNamara" within
105th Congress).
50. Id.
51. Presidential Nomination of Scott W. Muller, of Maryland, to be General Counsel of
the Central Intelligence Agency, PN2097-107, Rec'd by the 107th Congress, Sept. 3, 2002,
available at http://thomas.loc.gov/home/nomis.html (search "Scott W. Muller" within 107th
Congress).
we are not living in times in which lawyers can say no to an operation just to play it safe. We need excellent, aggressive lawyers who give sound, accurate legal advice, not lawyers who say no to an otherwise legal operation just because it is easier to put on the brakes. I also know that the lawyers assigned to the Directorate of Operations are not always perceived as part of a team by their clients but, rather, a hurdle that must be surmounted before the operators can do their jobs.\textsuperscript{52}

Senator Graham, a Democrat speaking to a Republican nominee, sought to ensure that Mr. Muller would not get in the way of the CIA’s operators.

In a dig at those who came before Muller, Senator Graham continued: “The previous General Counsel came before this Committee . . . and asserted that the officers in the Directorate of Operations needed adult supervision by their lawyers. As you might imagine, that comment was not well received at the Directorate of Operations.”\textsuperscript{53} From the context, it was not clear whether Senator Graham was referring to the interim General Counsel, John Rizzo, or to the prior Senate-confirmed General Counsel, Robert McNamara. To those at OGC, the “adult supervision” line sounded more like McNamara than Rizzo. In any event, Senator Graham sought a facilitator, a company lawyer, for the post-September 11 era. He seemed to suggest that oversight, whether external or internal, needed to have appropriate limits, and the lawyers should not interfere with the guardians who protect the United States from suicide bombers and weapons of mass destruction.

In that environment, Muller said enough of what Senator Graham wanted to hear. At one point, Muller declared:

I believe that the job of General Counsel of the Central Intelligence Agency is to provide timely, objective and independent advice to assist the DCI, the Agency, and the community as a whole in accomplishing their missions effectively and doing so in a way that is fully consistent with the laws and Constitution of the United States.\textsuperscript{54}

Muller thus adroitly straddled two of the General Counsel’s possible roles. He defined being labeled as either watchdog or lapdog. While he avoided the unfortunate “adult supervision” phrase, he included notes about independence and consistency with the laws. His view of the client included the head of the

\textsuperscript{52} Nomination of Scott W. Muller to be General Counsel of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence, 107th Cong. 2 (2002), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_senate_hearings&doid=f:83725.pdf.

\textsuperscript{53} Id.

\textsuperscript{54} Id. at 6.
CIA, the CIA itself, and the rest of the intelligence community. Muller also hit company notes with the phrase about “accomplishing their missions.”

Later in his testimony, in response to a question from Senator Rockefeller, Muller scored more points with Senator Graham:

I view the lawyer more as a navigator who will help the captains of the ship steer it as best they can so it’s not to hit shoals, to tell them where the water is deep and where it is shallow, and to give them their best judgment – my best judgment as to how the ship will fare in particular seas. But I will not be running it. I will not be the captain.\(^{55}\)

Here Muller revealed a lot. He would be on the ship to help the CIA navigate. He was not inclined to stay on shore, objecting on principle to any course the CIA had taken or would take. If the Committee did not seek too much supervision over the CIA, Muller was their man. On October 16, 2002, the Committee voted unanimously to confirm him.\(^{56}\) The full Senate confirmed Muller by voice vote the next day.\(^{57}\)

From his days at Davis Polk, Muller knew how to keep clients out of trouble. As the Agency’s General Counsel, he sought to keep the CIA out of trouble. During his tenure the CIA reportedly killed al Qaeda suspects through Predator strikes, interrogated al Qaeda prisoners more aggressively than allowed in the criminal justice system, and shifted suspects to secret prisons all over the world. It is impossible to know what advice, if any, Muller gave the Agency concerning these actions. But if he approved any of them, some might say he sought to protect the Agency more than the public interest. Others would argue that the public interest was well served. Whether or not Muller kept the CIA out of trouble remains to be seen.

Long before al Qaeda appeared on the scene, the United States faced serious threats. For much of the Cold War, the nation directly confronted a Soviet adversary that could assure its destruction. The United States fought long wars in Korea and in Vietnam. And it battled the Soviets through proxies in Africa, Latin America, and Asia. Even against these ultimate threats, not all General Counsels at the CIA were lapdogs.

The CIA’s first General Counsel, Lawrence Houston, openly questioned whether the CIA’s fifth function under the National Security Act of 1947\(^ {58}\) included paramilitary actions, separate from gathering foreign intelligence. That did not make him popular with all the operators bent on covert action. But even for a facilitator that was principled advice.

\(^{55}\) Id. at 11.

\(^{56}\) Id.

\(^{57}\) Id.

\(^{58}\) The so-called “fifth function” is described in §102(d)(5) of the 1947 Act, now codified at 50 U.S.C. §403-4a(d)(4).
More recently, Daniel Silver, the CIA’s General Counsel from 1979 through 1981, held a reasonable view of what the CIA’s top lawyer is supposed to do. Consistent with this article’s interest in internal checks, he noted that “the first bastion of oversight is within the intelligence agencies.”

As between the Inspector General and the General Counsel, Silver suggested that the General Counsel could do a better job of preventing misconduct. Silver identified several requirements that must be met if lawyers are to be effective at CIA, criteria that are as relevant today as they were when Silver was writing in the wake of Iran-Contra. First, the lawyers must be “independent” and “strong-minded.” Second, the Agency should respect the rule of law by keeping its lawyers involved in sensitive activities that have “flap potential.” The lawyers should view themselves as more than the DCI’s personal lawyers, but they should not go so far that the operators view them as “adversaries.” They need, in a word, balance.

Silver recognized that it is difficult for the General Counsel to maintain a proper balance. His views thus overlap mine. While Silver did not use this article’s canine designations, he was optimistic that a General Counsel could be bred and trained who would be somewhere between a watchdog and a lapdog. He was all for hybrids.

In the aftermath of Iran-Contra, Silver was not analyzing the role of the CIA’s General Counsel for pure academic pleasure. His goal was to head off what he considered overly intrusive proposals for congressional oversight. Back then, he had a vested interest, and, as a counter to proposals being considered on Capitol Hill, he may have exaggerated the effectiveness of internal checks on Agency misconduct. He was probably behaving more as an advocate than as a scholar. That is understandable, because the line between advocacy and scholarship, in his article as in mine, is not always clear.

In 2007, Acting General Counsel John Rizzo, in advance of public statements in a confirmation hearing, responded to questions about the lawyer’s function in the intelligence community. Rizzo said, optimistically, that he does not believe in a “disconnect” between the CIA’s interest and the


60. At that time, Silver was comparing the General Counsel to a prior version of the Inspector General. Id. Unlike the current Inspector General, the prior one was not created by statute and did not have a dual reporting line to the DCI and to the congressional oversight committees. In short, the Inspector General has changed since then. See 50 U.S.C.A. §403q (West 2003 & Supp. 2006).


62. Id. at 14.

63. Id.

64. See Check, supra note 43, app. at 15, 21, 25.
public interest." Further, he sees himself as a watchdog at the Agency. In fact, Rizzo claimed, "on those isolated occasions over the years" when the CIA’s management has criticized the General Counsel, "it was because of a perception that the GC was not being sufficiently rigorous in this oversight role." Rizzo believes the General Counsel must go beyond strictly applying facts to legal standards; he would counsel against something that is "strictly legal but nonetheless imprudent or untimely." He would factor in the reality of Washington politics. Whether Rizzo has actually lived up to his own declared standards is difficult to answer, especially for those who lack access to information about his earlier performance. All the same, his comments for public consumption give some sense of his ideals.

Rizzo finally had his confirmation hearing on June 19, 2007. Seven Senators attended this hearing, five Democrats and two Republicans, a better turnout than at Scott Muller’s hearing in 2002. Rizzo’s opening statement accepted the importance of external oversight, drawing lessons from Iran-Contra. But instead of exploring deep issues of internal oversight with Rizzo, the Senators spent much of their time during the two-hour open session posturing about extraordinary rendition and the CIA’s detention and interrogation program.

C. Other Views

Aside from the General Counsels themselves, senior officials at the CIA have not said much on the public record about OGC’s role in internal oversight. DCI Woolsey, as noted, lobbied against making the General Counsel subject to Senate confirmation. Otherwise, internal oversight has not generated much commentary by the operators. Senior officials at the CIA, positioned somewhere between neglect and disdain, leave intricate legal issues to the lawyers. In a memoir of more than five hundred pages, former DCI George Tenet includes not a single page about OGC or the General Counsel; neither Scott Muller nor John Rizzo is named.

IV. GETTING IN AND STAYING IN

The CIA’s General Counsel is selected through a political process, while other lawyers in OGC are selected through a bureaucratic process. For both

65. Id. app. at 15. Rizzo further noted, “I have always felt as a CIA lawyer it is not only possible but essential to conduct oneself in a way that simultaneously protects the Agency’s and the public interest.” Id.
66. Id. app. at 25.
67. Id. app. at 21.
68. See supra text accompanying notes 35-37.
the General Counsel and her staff, staying in the OGC may be as difficult as getting in.

A. The Application Process

OGC employs about 100 lawyers. Entry-level lawyers are called Attorney-Advisors. The next level is Assistant General Counsel. The most senior level, aside from the General Counsel and her Deputy, is Associate General Counsel.

Applications for jobs at the CIA from lawyers and others have skyrocketed since September 11, 2001. The tragic attacks on the American homeland caused a surge of patriotism and a renewed call to public service. An Agency that wondered what to do after victory in the Cold War now has a clear mission. No longer does Senator Frank Church display the Agency’s misdeeds to the cameras. No longer does Senator Patrick Moynihan call for the CIA to be disbanded. Boycotts and protests against the CIA have, for the most part, disappeared. Americans are now more afraid of terrorists than of their own government.

As Sixties radicalism has been replaced by careerism, students apply to the CIA on-line and through the mail. They line up proudly for interviews with CIA recruiters on campus. The CIA is now part of their popular culture, thanks to television programs such as Alias and 24. Even Hollywood stars cannot resist the intrigue. Both Ben Affleck and Robert DeNiro have been to CIA headquarters, preparing for roles and doing research on film projects. Affleck was at Langley for The Sum of All Fears, and DeNiro was there for The Good Shepherd.  

CIA’s OGC has benefitted from the surge in public support for activities on the dark side of American policy. The office has hundreds, if not thousands, of applications for a handful of openings each year. For the intelligence community, it is a buyer’s market for legal talent.

1. Honors Attorneys and Laterals

OGC hires through two channels, an honors program and a lateral program. The honors program is open to attorneys with up to three years of experience, while the lateral program is open to those with more experience.


71. When a senior official introduced DeNiro to John Rizzo in a long hallway, the actor, shocked to find out that the CIA employed lawyers, could think of nothing more to say than to comment on Rizzo’s “nice threads.” Rizzo confirmed these details during a visit to my law school on March 28, 2007.
The honors attorneys, many of whom come to OGC straight from judicial clerkships, rotate among various OGC divisions during their three-year program. Most honors attorneys, if interested, are allowed to stay in OGC.

It is rare for OGC to hire a lateral attorney with more than five years of experience. Those who are hired with five or more years of experience usually come from other government agencies. Moreover, OGC is reluctant to hire attorneys who have been trained in a different professional environment, such as a legal services office or a public defender’s office. If challenged about this, OGC might point to a steep learning curve about intelligence issues. Another reason may be the conscious or unconscious need for conformity in the ranks.

2. The Advertising Campaign

OGC has played up the cult of intelligence in its advertising. When I applied to OGC, the CIA’s website and brochures had reprinted a section from a 1999 book called America’s Greatest Places to Work with a Law Degree. This book quotes unnamed OGC lawyers who are proud of their work, which they describe in positive terms: “excitement,” “cutting-edge,” “fascinating,” “nitty-gritty.” While stirring up images of James Bond, the book halfheartedly advises candidates, “Don’t get too carried away with the shoe-phone and lapel camera stuff!”

OGC targets disgruntled law firm associates and law students whose summer experiences were not all thrills. OGC’s website asked, “Who would you rather work for?” One side, we are told, has Mont Blanc pens. The other side has ballpoints. If the candidate is still interested, she is reminded that the normal place has 2600 billable hours. The special place has ten federal holidays and, depending on the employee’s years of government service, between 13 and 26 days of annual leave.

Federal holidays may appeal to candidates who seek a gentler lifestyle, but the main attraction is the myth of James Bond. When I applied, the special place offered the possibility of “globe-trotting,” being a “footnote in history,” spending a “weekend in Paris,” meeting a “contact late at night in unfamiliar surroundings,” and having a “day measured in time zones visited.” For candidates bored with marking up proxies and coordinating document production, the intrigue may be more than they can resist. If, during interviews at OGC, a current lawyer tells a candidate that the work is not so glamorous, she may consider this a trick to impede access to the inner sanctum. Once upon a time, they were lured by multi-million dollar deals and multi-district litigation. Now they are lured by espionage.

Only Madison Avenue would take pride in such advertising. The truth is that an OGC lawyer is more likely to spend a weekend in Paris on vacation.

than on business. She must be willing to trade a high income in a law firm for work she hopes will be meaningful. She must want to do her part in making America safe. She needs to know that the CIA's General Counsel makes important decisions, and that OGC is important. In fact, OGC should not and need not perpetuate fantasies in order to attract good staff lawyers. It would still be able to recruit and retain good candidates if it told the truth.

Some OGC lawyers become disgruntled with the truth after a few weeks working on Freedom of Information Act requests. Even so, their dissatisfaction does not result in many defections from OGC's ranks. Both the candidate and the Agency have made substantial emotional and financial investments in their placement. The departures that do occur are often from the junior ranks, by lawyers frustrated by the slow progress toward increased responsibility and by the low pay.  

3. The Clearances

Non-conformists need not apply to the CIA. To be eligible for employment, an OGC lawyer must obtain a Top Secret clearance. This clears the lawyer for information the disclosure of which might cause "exceptionally grave damage" to the national security. In addition, the lawyer must be cleared for "sensitive compartmented information."  

The cost of clearing a lawyer comes from OGC's own budget. Because the clearance is expensive, OGC weeds out candidates who are likely to use the lawyer's track to pursue other CIA opportunities. Of those not weeded out, a lawyer who transfers to other parts of the CIA is a tangible loss for OGC. Of those who do transfer, many go to the Directorate of Operations as intelligence officers. During my tenure at OGC, two junior lawyers transferred to the DO, only to be scolded by John Rizzo. Before that, another OGC veteran, also unpopular with Rizzo, had gone on to head the Special Activities Division and later the Counter-Intelligence Center. This veteran, later explaining his transfer out of OGC, said to me that he was "tired of handing out towels at the game." Nevertheless, most lawyers are content to work on the sidelines.

---

73. I took special notice of those who attended the same law school I did. One honors attorney who had clerked for a federal appellate judge left for a United States Attorney's Office. Another left to join a D.C. law firm.


75. SCI is not a higher clearance than TS. Imagine SCI as a folder within a filing cabinet labeled TS. A common example of an SCI compartment is a particular covert action. In order to receive information that is classified Top Secret and also designated SCI, the recipient would need to hold a Top Secret clearance and also any SCI clearances that are pertinent.
OGC uses a standard government form for security clearances. The form is long, calling for details about prior residences, prior employment, academic credentials, financial history, and foreign travel. The CIA’s background investigators, working from the applicant’s completed form, will review, at a minimum, the applicant’s credit history and will check to make sure that she does not have problems with the Internal Revenue Service. The background investigators, not necessarily revealing that they are checking a CIA applicant, will also interview the applicant’s friends and acquaintances.

During the background investigation, the CIA takes an intimate look into the candidate’s life. The anticipation of such an inquiry deters some people from even applying. Some candidates, who place a higher value on their privacy than they realized at the beginning of the application process, do not continue with the investigation. Of those who continue, some are cleared and some are not.

If a candidate has more than a casual relationship with any foreign nationals, she must list their names, addresses, and telephone numbers. This listing gives the CIA a chance to check the foreign nationals against various intelligence databases. If one of these names leads to a hit, for example, as a known intelligence officer, it will provoke additional questions during the security interview. Too many hits may doom the candidate’s application.

In the old days of CIA recruiting, homosexuality served to exclude a candidate. That has changed since one CIA employee, a covert electronics technician, was fired because of his homosexuality. Rather than go away quietly, the employee challenged the firing. The Supreme Court held that “Mr. John Doe” presented a colorable constitutional claim that was not precluded by the DCI’s prerogatives under the National Security Act. Partly as a result of this decision, the CIA no longer discriminates openly against homosexuals.

Whether there is hidden discrimination against homosexuals at the CIA is difficult to tell, since the background investigation remains a mystery even to those who receive clearances. What is clear is that I encountered a much smaller proportion of people at the CIA who were openly homosexual than I have seen elsewhere in my career as a lawyer.


77. Because of my contacts with Iranian officials while I ran the U.S. Chamber of Commerce’s Iran Commercial Initiative, it took me more than two years to obtain a clearance.


Whether there is hidden discrimination against other minorities—African-Americans, Muslims, or Jews—is also difficult to tell. But my wife mentioned on her two visits to CIA headquarters, one on "family day" and another for my going-away party, that the place had the feel of a suburban shopping mall in her native Missouri. In addition, a former CIA case officer states that the CIA is not friendly to women.

4. The Polygraph and Other Tests

All successful candidates must pass a polygraph examination. The CIA also uses the machine to update the security clearances of employees every five years or so. Although polygraph results are not considered reliable enough for use in federal courts, the CIA places great faith in them. The CIA's confidence is so well known that Hollywood movies have noted an American penchant for "fluttering" people. Our British "cousins," it seems, look to other signals in background investigations.

The more examinees believe in the machine, the more effective it is said to be. Presumably as a result, conversations between CIA examiners and subjects who are or who will soon be hooked up to the machine often produce more information than the machine's readings. Because candidates believe in the machine's ability to identify misstatements and evasions, they disclose information that they might otherwise withhold.

Not all agencies share the CIA's faith in the machine. Use of the polygraph is not as prevalent in the Department of Defense, except within the National Security Agency. Within the Justice Department, the FBI, responding to the Robert Hanssen spy scandal, uses the polygraph to trim potential traitors from the mass of its applicants. In addition, the FBI sometimes uses the machine on informants and cooperating witnesses.

Besides passing the polygraph, OGC candidates, as potential watchdogs and lapdogs, must be in good health. Like all CIA candidates, they must obtain a medical clearance. The examination for a clearance includes blood work, a chest x-ray, a vision and hearing test, and an EKG. Some basic psychological testing, along with a short interview with an examiner, is also done to sort out the insane and the seriously troubled. (Candidates for the

80. Adam Cianfili, a former OGC staff lawyer, filed suit against the CIA, accusing OGC of discriminating against him because he is Jewish. See Vernon Loeb, Back Channels: The Intelligence Community; Cold War Spies to Compare Notes in Berlin, WASH. POST, Sept. 10, 1999, at A35; Janine Zacharia, Fired Jewish CIA Man Asks Clinton, Gore to Intervene, JERUSALEM POST, Sept. 3, 2000, at 5.

81. See Melissa Boyle Mahle, Denial and Deception: An Insider's View of the CIA from Iran-Contra to 9/11 (2006), at 124.

82. See The Russia House (MGM 1990). "FLUTTER" was a memorable element of the CIA cryptonym for the polygraph.
clandestine service undergo more detailed testing. A candidate's urine is also tested for medical problems and for indications of illegal drug use.

One mysterious aspect of the background investigation is the question of what sort of illegal drug use is disqualifying. Dealing drugs is of course worse than using them. The more recent the use, the more it is a problem. Use of Yuppies drugs like marijuana and cocaine is less of a problem than heroin or LSD. In any event, the Office of Security keeps the candidates guessing, as "suitability" decisions are made on a totality of factors. That is part of the reason it is next to impossible for candidates to succeed in challenging denials of a clearance, whether through internal appeals or in the courts. The DCIA is charged by the National Security Act to resolve any doubts about a clearance against the candidate and in favor of national security. 84

By design, the Office of Security is risk averse. A security bureaucrat is not punished for turning away great candidates. On the other hand, a bureaucrat may suffer for being part of a process that approves someone who eventually turns out to be a traitor. Imagine the consequences for the examiner who let Aldrich Ames, the CIA turncoat, talk his way past indications of deception during a polygraph examination.

In my view, the CIA needs to break away from its traditional aversion to risk if it is to more effectively carry out its functions. Otherwise, fine lawyers, analysts, and case officers will continue to be turned away unnecessarily, and it will be difficult for OGC and the rest of the Agency to expand their perspectives. For the sake of national security, particularly in the battle against radical Islam, the CIA should open its doors to candidates who are immigrants and the children of immigrants, even those candidates who are more difficult to get through the clearance process. Learning a foreign language at a CIA training center is not the same as learning that language as a native. Learning a foreign culture in a U.S. school is not the same as living that culture. Only so much can be done to make Middle Americans fit into the Middle East and other hard-to-penetrate areas, making it imperative for the CIA to give fair consideration to capable candidates, even if they have backgrounds that traditionally have set off warning bells in the Office of Security.

5. Inter-Agency Comparisons

A revolving door exists between the military and the CIA, although more lawyers go from the military to the CIA than the other way around. Many at

83. I know this first-hand from my application for a position as an intelligence officer in the DO.
84. 50 U.S.C. §403-4a(e)(1) (Supp. V 2005) ("[T]he Director of the Central Intelligence Agency may, in the discretion of the Director, terminate the employment of any officer or employee of the Central Intelligence Agency whenever the Director deems the termination of employment of such officer or employee necessary or advisable in the interests of the United States."). The CIA has a corresponding internal regulation on security clearances.
OGC served earlier as military lawyers. While at the CIA, some of these lawyers are given paid leave for military training that keeps them in reserve status. Some retire from the military before joining OGC, enabling them to draw both an OGC salary and their military stipends and pensions.

The military influence at OGC leads to the use of expressions—such as “roger that” and “stand down”—that annoy some who have not worn a uniform. Other civilians, wittingly or not, adopt the military lingo. All in all, the military marks the CIA more than the CIA marks the military.

While the lawyers in OGC are qualified, they do not stack up against the Justice Department’s elite cadre of attorneys. Not many OGC lawyers come from Justice, although a few OGC lawyers eventually transfer there. Compared to the Office of Legal Counsel or to the Solicitor General’s Office, OGC has fewer lawyers who attended top-ten law schools, served on law reviews, or clerked on a federal appellate court. Supreme Court clerkships are not common credentials at OGC, as they are in the Solicitor General’s office. With about 100 lawyers, it may be difficult for OGC to develop or to maintain elite standards. Slow turnover contributes to stagnation. By comparison, the Office of Legal Counsel and the Solicitor General’s Office are each a fraction of OGC’s size. Accordingly, a fairer comparison might be between OGC lawyers who serve in the COI and lawyers in Justice’s most selective components. Even by that comparison, however, OGC does not measure up. In sum, OGC is a place for good lawyers, not great lawyers.

The Justice Department and the CIA are two different clubs. At Justice, lawyers are the center of attention, with the Attorney General at the top of the chart. It is a lawyers’ club. The CIA is a spy club. The lawyers are off to the side, and OGC occupies a small box on the organizational chart next to the DCIA. Some OGC lawyers try to compensate by aping the surrounding culture. Some even outdo the analysts and case officers in using spy lingo. Other OGC lawyers just make do.

B. Ongoing Scrutiny

Even after an OGC candidate is cleared, scrutiny continues. As with most clubs, payment of dues follows initiation fees. Once the OGC lawyer receives her coveted blue badge as a full-time employee, she is required to fill out regular notifications and reports. Thus, she spends some of her energy keeping the Office of Security happy. As a company woman, it is difficult, if not impossible, for her to be an iconoclast. While she watches over the case officers and analysts, the Office of Security watches over her—a guard over the legal guardian.

Still, the security watch at CIA is less intrusive than at intelligence services in other countries. Diplomats and intelligence officers from non-democratic countries are accustomed to “minders” who accompany them to make sure they do not go over to the other side. The Iranians, for example, do not leave their officials alone for long, abroad or at home. Their minders, like human blankets, join the officials in restaurants, hotel suites, even restrooms.
On the other hand, CIA officers do not believe that someone is always watching over them. At home, unless they have fallen under some serious suspicion, they assume that the Office of Security is not monitoring their phone calls, emails, and personal activity. They take their children to soccer games without another set of watchmen monitoring them.

1. **Classified Information**

CIA lawyers are not allowed to share classified information with people who lack authorized access. In forming legal opinions based on such information, CIA lawyers are not allowed to consult lawyers outside the government or to consult lawyers within the government who have not been “read into” a relevant classified compartment. For this reason, writing a legal document at OGC is different from writing scholarly articles that benefit from a wide range of comments and critiques.

Only a few people will review the quality of an OGC lawyer’s work. OGC does not publish its legal opinions, and the OGC work-product that is published is usually subsumed into a Justice Department filing. Many commentators, using the Justice Department’s August 2002 “torture” memorandum as evidence, have concluded that the best legal analysis does not take place in such secrecy.

Ciphör locks, special phones, and classified fax machines add to the CIA lawyer’s chores. CIA lawyers work in vaults where they can leave classified documents out on their desks, relying on the last person out for the day to lock the vault to bar access from other parts of the CIA. Lawyers who work on more sensitive projects have separate safes in their offices, to prevent other lawyers from peeking at documents related to such projects. The safes are compartments within compartments, another impediment to comprehensive oversight.

CIA lawyers are not allowed to share secrets with their spouses, children, or other family members. As a result, a legal guardian at the CIA may be lonely. Even if family members have security clearances, even if they work at the CIA, the odds are that they do not have the requisite need to know. Sometimes the CIA’s very connection to a matter is classified. When a CIA lawyer makes a trip on such a matter, the most she may tell her spouse is the city she is visiting. Clever spouses, of course, can sometimes connect the city to high-profile litigation; even the Office of Security must resign itself to accept such leaks. CIA lawyers are not, after all, trained operatives. Theirs is not the business of dead-drops and chalk-marks.

2. **Financial Disclosure**

All CIA employees, including lawyers, fill out a financial disclosure form on an annual basis. This multi-page form calls for information about assets and liabilities, reaching such details as what kinds of cars the employee owns, whether the employee leases or owns her home, and what the employee’s
outside sources of income are. The financial reporting requirement is a direct reaction to the Aldrich Ames spy scandal. Ames’s conspicuous consumption — fancy suits, new teeth, a Jaguar, and a house paid for in cash — did not draw sufficient attention from the CIA’s Office of Security.\(^5\) Today’s CIA employees pay for Ames’s sins with additional paperwork, another sign that all the watchmen are watched.

Of course, an employee who is willing to commit espionage will not hesitate to lie on the financial disclosure form. Even so, if an espionage prosecution of the employee encounters problems of proof or sensitivities about sources and methods used in the investigation, those false statements provide an alternative means of prosecution. A false statement prosecution\(^6\) is more straightforward than a prosecution under statutes that turn on complex definitions of “national defense” information\(^7\) and on the intent to help a foreign power. Thus, the CIA’s paperwork is not completely unnecessary.

3. Outside Contacts

In my experience, all lawyers at OGC were overt. They were not required to hide the fact of their employment by the CIA. Nevertheless, some of us, in the tradition of CIA analysts, were discreet about our employment, not wanting our prior contacts and former employers to become subject to outlandish speculation that they were CIA fronts. Further, although the 9/11 tragedy has caused a renewed respect for public institutions, the CIA is still not popular in all quarters.

Whether CIA employees are overt or covert, some requirements are universal across the Agency. For example, OGC lawyers are not allowed to speak to the media without prior authorization. Indeed it would be very unusual for OGC lawyers to receive such authorization, since the CIA’s official interaction with the media is most often funneled through its Office of Public Affairs.

Leaks, however, can occur in any part of the CIA or elsewhere in the intelligence community. Preventing and plugging leaks are perennial problems, and, as demonstrated by the firing of Mary McCarthy at the Office of Inspector General,\(^8\) there may be harsh consequences for those who have unauthorized contacts with the media.

OGC lawyers must notify the Office of Security concerning their contacts with outside organizations and their personal plans to travel overseas. The purpose of these notifications is to steer lawyers away from situations where


\(^88\) Mark Mazzetti & Scott Shane, C.I.A. Defends Officer’s Firing in Leak Case, N.Y. TIMES, April 26, 2006, at A17.
they may be assessed, developed, or pitched by foreign intelligence services and to guide them away from awkward or inappropriate interactions. Another purpose of the notification about foreign travel is the lawyer's safety. CIA officers in the field will keep a non-operational employee away from active operations, and in emergencies CIA officers might even look out for her. Some CIA employees, rather than bother with the paperwork and subject colleagues to unnecessary scrutiny, stay away from outside organizations and opt for domestic travel. Such decisions contribute to the isolation of OGC lawyers from their communities.

Even overt employees from headquarters, such as OGC lawyers, travel overseas under light cover. That is as close as most of them get to tradecraft. To avoid hostility, they do not discuss their true employment. Cover also helps to keep them clear of surveillance from foreign services.

At home or abroad, everyday interactions of the OGC lawyer may contain the seeds of espionage. Imagine that she is about to become involved in a school board in Arlington County and, unbeknownst to her, but known to other parts of the CIA, a member of the Russian foreign intelligence service has joined the board. She may be setting herself up for a pitch.

If a lawyer believes that a neighbor or acquaintance has been too inquisitive about her career, she is expected to report that to OGC's security officer. Once the security officer checks the appropriate CIA databases for information about the individual with whom the OGC lawyer has had contact, he will advise the lawyer on her next steps. In most cases, the advice will be to avoid or to minimize contact. It is conceivable, however, that U.S. operatives might turn the contact around. The OGC lawyer might then function as a double-agent or might facilitate a pitch to somebody on the other side. She might be lucky enough to play out her spy dream. Anything is possible.

On balance, the personal life of an OGC lawyer is not much different from the lives of other Washington bureaucrats. She shops, practices yoga, and sees movies in the usual places. Yet as a result of the CIA's security requirements, she is more on guard about casual encounters. What may be uneventful for a lawyer in the Department of Labor may be more significant for someone in the intelligence community. So she develops a suspicion about her surroundings, learns that things are not always as they appear on the surface, and sometimes sees complications where there is utter simplicity. For better or worse, her OGC career changes her.

89. For example, they might include her in plans to evacuate U.S. personnel.
90. I resigned from my board position with the Iranian-American Bar Association, and I discontinued my affiliation with the American Iranian Council.
C. Justice Department Interaction

OGC lawyers deal with matters both inside and outside the Agency. Inside, they advise on government ethics (for example, whether an employee may accept the gift of a saber from a foreign intelligence service), and they handle administrative appeals (for example, discrimination claims by employees). This aspect of OGC practice has much in common with the ethics and administrative practices at other agencies. The details of the working environment are different, but, for the most part, the rules and regulations are the same.

Also in line with other general counsels' offices, OGC has outside interactions with the Justice Department regarding litigation. OGC's Litigation Division is the most active communicator with the Justice Department.91

If CIA information is involved in litigation or in potential litigation, OGC lawyers become involved as early as possible. Their mission, quite simply, is to protect the CIA's information from disclosure. They attempt to do so without unnecessarily compromising the work of the rest of the United States government. CIA information can be drawn into both civil and criminal cases. The more the CIA classifies, the more its information will be drawn into both kinds of cases.

One task of OGC in a civil case may be preserving the cover of a CIA employee without making false statements. The secrets must be protected while justice is done. Imagine an inflamed divorce proceeding in which a spouse knows the CIA employee's true occupation but those outside the classified realm do not, a traffic accident that involves a covert CIA employee in a government vehicle, or an airplane crash into a secret CIA facility. The possible variations are endless.

I. State Secrets Practice

Whether or not the United States government is party to a civil lawsuit, the CIA sometimes needs to assert the state secrets privilege. According to the case law, the state secrets privilege is not to be "lightly invoked."92 It can only be asserted by the head of the agency with control over the matter after personal consideration.93 During my tenure at the CIA, the DCI asserted the privilege on behalf of the Agency. After creation of the National Directorate

91. I served as a senior attorney in the Litigation Division. OGC also has an Operations Division, an Administrative Law Division, a Contract Law Division, and an Intelligence Support Division, along with legal advisors to the CIA's chief financial officer and the chief information officer.


93. Id. at 8.
of Intelligence, both the DCIA and the DNI should have this authority. In practice, it seems that the DCIA continues to assert the privilege for the CIA.\footnote{See El-Masri v. Tenet, 437 F. Supp. 2d 530, 535 (E.D. Va. 2006), aff'd, 479 F.3d 296 (4th Cir. 2007), cert. denied, 128 S. Ct. 373 (2007) ("In support of its formal claim of [state secrets] privilege the United States submitted both an unclassified and a classified ex parte declaration of the Director of the CIA (DCI).".)}

When questions arise about state secrets, OGC lawyers consult with their counterparts in the Justice Department's Civil Division. With policy and law stirred into the mix, they determine whether the privilege should be asserted. If the lawyers decide an assertion is necessary, they will draft a memorandum to the DCIA that explains the case and recommends the privilege. This memorandum, along with the necessary affidavits, will go through the General Counsel.

The DCIA, a political appointee, takes assertions of the state secrets privilege seriously. He consults with his staff to weigh the political implications of any assertion. An unclassified affidavit asserting the privilege is usually filed on the public record in the case, and a classified affidavit goes only to the court. If the CIA’s connection to the case is itself classified, the privilege will need to be asserted in a way that does not mention the Agency. One solution is for the head of another agency, as a party to the suit or as an intervening party, to file the unclassified affidavit and for the DCIA to file the classified affidavit. After the privilege has been asserted and upheld by the court, the litigation either works around the secrets or is dismissed.

2. Totten Practice

OGC lawyers also handle cases that involve the Totten doctrine, but these arise less often than state secrets cases. Totten recognizes a prudential bar for courts asked to hear cases that involve secret agreements for secret services. The Totten doctrine was articulated in a case in which William Lloyd entered into an agreement with President Abraham Lincoln, for a monthly salary and expenses, to spy behind Confederate lines during the Civil War.\footnote{"Both the employer and the agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter." Totten v. United States, 92 U.S. 105, 106 (1875).} The Supreme Court ruled that Lloyd’s claim, brought by the administrator of his estate, was nonjusticiable. More than a century later, the Supreme Court reaffirmed the Totten bar when it dismissed a lawsuit by two alleged spies from a Cold War adversary against the CIA for breaching a promise to take care of them for life.\footnote{Totten v. Doe, 544 U.S. 1 (2005).}

Using an invigorated Totten doctrine, OGC lawyers may now try to convince courts to dismiss other kinds of cases without submitting affidavits and without asserting a privilege.\footnote{See A. John Radsan, Second-Guessing the Spymasters with a Judicial Role in Espionage Deals, 91 IOWA L. REV. 1259, 1291-1295 (2006).} They may also use Totten to bolster...
requests to dismiss cases involving state secrets. In the new Totten era an internal guard (OGC) works against a weakened external guard (the courts), and more and more of the CIA’s information is kept secret.

3. FOIA

Although the CIA is not immune from Freedom of Information Act requests, it benefits from many protections. For instance, the CIA generally is not required to search its operational files in response to a FOIA request. All the same, the documents pile up in the directorates, and the Agency must separate the documents that stay inside the building from those that must be turned over to outside requesters. As for documents that are not operational, the CIA makes ample use of Exemption 1 (for information that has been properly classified) and Exemption 3 (for information “specifically exempted from disclosure by statute”).

CIA classifications are subject to more second-guessing under FOIA than they are under state secrets and the Totten doctrine. Perhaps the courts are more assertive in FOIA cases because they consider the stakes to be lower, and in any event the procedural context is more favorable for FOIA requesters. Despite the differences, the flow of FOIA records to outsiders is more of a trickle than a stream.

CIA lawyers review the assertions of FOIA exemptions for documents and categories of information. They coordinate with lawyers from other U.S. agencies whose documents may have come into the CIA’s possession, prepare the Vaughn indices (a correlation of FOIA exemption claims with the information withheld), and draft the motions in FOIA litigation. In FOIA cases, the internal guardians at OGC justify CIA decisions to external guardians—Justice Department lawyers and the federal courts. At other times, OGC lawyers counsel CIA officials to back away from unreasonable classifications. This is one area in which they perform meaningful oversight.

4. CIPA Basics

The Classified Information Procedures Act (CIPA) creates another arena in which CIA classifications are second-guessed, another area for oversight.

---


99. See Winchester & Zirkle, supra note 98, at 236.

100. See id. at 250.

101. See 5 U.S.C. §552(4)(B) (in a FOIA case, the district court “shall determine the matter de novo, and may examine the contents of . . . agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions . . . and the burden is on the agency to sustain its action”).

2008] QUIS CUSTODIET IPSOS CUSTODES AT THE CIA? 233

When the Justice Department is sufficiently aligned on a case with the CIA, it considers its discovery obligations (under Brady, Giglio, Jencks, and Rule 16 of the Federal Rules of Criminal Procedure) to extend to CIA files. Alignment often occurs in terrorism and espionage cases. Alignment has also occurred in narcotics cases and in prosecutions under the Foreign Corrupt Practices Act. When alignment exists, the Justice Department asks the CIA to search its files for information related to the case. Even if alignment does not exist, the Justice Department may ask for a “prudential search” to determine whether witnesses in the case have any connection to the CIA or whether any truth exists in a defendant’s claim (such as that made by Manuel Noriega) that the CIA put him up to committing his crime.

In theory, Main Justice is supposed to coordinate all CIPA requests from the Justice Department, but in practice a prosecutor’s office that is accustomed to dealing with OGC often makes its requests directly. This is most likely to be done by the offices of the United States Attorneys for the Eastern District of Virginia and for the Southern District of New York, which have had OGC contacts from prior terrorism and espionage cases. While I worked at the CIA, OGC did not object when Main Justice was bypassed in this way, perhaps to the chagrin of DOJ’s Counter-Terrorism Section and the Counter-Espionage Section, two sections that are now part of a new National Security Division. In my experience, OGC enabled Justice Department superstars to work around Main Justice, a practice that may continue to this day.

Since 9/11, CIPA has become better known to the public. In the Moussaoui case, for instance, CIPA was applied by analogy to a situation that


did not directly involve classified documents, but rather the defendant’s request for access to high-level al Qaeda detainees. Moussaoui claimed that those detainees would exculpate him or mitigate his role in the 9/11 plot. By the sentencing phase, Moussaoui was provided with detainee statements but not with personal access to the detainees themselves. In another case, OGC lawyers were surely busy interacting with special prosecutor Patrick Fitzgerald in the prosecution of Scooter Libby.

Contrary to popular myths, OGC lawyers do not simply push a button to respond to the Justice Department’s CIPA requests. Instead, those lawyers pass the requests on to other people in the Agency, and CIA experts outside of OGC search various databases for the requested information. Some of the databases are so old that they must be searched manually. Because the searches are as much art as science, it is difficult (if not impossible) to guarantee that all responsive documents have been gathered. This difficulty applies to internal searches, too. The motivation of the CIA searchers may differ, depending on whether the request is internal to the CIA—part of an operation—or external. Enthusiasm may run higher for CIA-initiated searches than for those being conducted at the behest of other government agencies, so one oversight role for OGC is to push the searchers to be consistently diligent.

The bulk of what the searchers gather is CIA cables. Once the cables have been gathered, a prosecutor with an appropriate security clearance (for example, Patrick Fitzgerald) is allowed to review them at CIA headquarters. An OGC lawyer coordinates this review. A thorough OGC lawyer reviews the documents before the prosecutor does. A less thorough OGC lawyer just makes sure the stack is in the right place. If the prosecutor determines that nothing needs to be turned over to the defense, the CIA’s role usually ends there.

5. CIPA Abuse

If nothing is turned over to the defense, it is unlikely that a defendant will ever learn about the search of CIA files. Although the Justice Department’s search request is not by itself classified, any response from the CIA, negative or positive, is almost surely classified. Revealing what the CIA does not know (for example, concerning a terrorist group) or does not have an interest in (for example, satellite imagery of a certain country) may create as much damage as disclosing the contents of CIA cables. OGC will not tell the defendant about the search on its own.

A skeptic might ask whether there is any check on a prosecutor who sees discoverable information at the CIA but does not acknowledge it. Will OGC second-guess the Justice Department’s decision that something need not be turned over? Will one agency watch over another?

Since OGC lawyers have enough trouble finding an appropriate role—between watchdog and lapdog—in their interactions with CIA officers, they do not seek out additional battles with prosecutors. In dealing with the Justice
Department, OGC is the entity that crs toward non-disclosure. OGC lawyers consider their duties to be separate from the prosecutor's duties, viewing Brady and other discovery rules as the Justice Department's problem, not the Agency's. Whether this view is correct has, like much of OGC's work, not been closely analyzed or tested in the courts.

Fereting out a prosecutor's misconduct, in ordinary cases and in national security cases, is difficult but not impossible. One case that warrants optimism about oversight - even in CIPA cases - is the Koubriti prosecution in Detroit. There, four persons were indicted for allegedly being part of a post-9/11 sleeper cell. The convictions were overturned after trial because of prosecutorial misconduct. Part of that misconduct, which the Justice Department brought to the court's attention, related to a drawing in a notebook that was found when the defendants were arrested. An expert witness for the prosecution - an FBI supervisor - testified that the drawing was a sophisticated casing of a terrorism target in Turkey. What the prosecutor did not reveal was that during a review before trial a CIA expert did not consider the drawing to be so sophisticated. This difference of opinion between government experts, which was not revealed to defense lawyers until after trial, might have served the defense well in cross-examination at trial.

During the Justice Department's own internal investigation into the misconduct in Koubriti, the prosecutor filed a civil suit against then-Attorney General John Ashcroft and others, alleging that he was being made a scapegoat for blowing the whistle on the government's incompetence. Eventually, the prosecutor was prosecuted for his handling of the Koubriti case but was acquitted. Defendant Koubriti later filed a damage suit against


107. United States v. Koubriti, 336 F. Supp. 2d 676, 679 (E.D. Mich. 2004) ("[T]he prosecution materially misled the Court, the jury and the defense as to the nature, character and complexion of critical evidence that provided important foundations for the prosecution's case. As the Government's filing also makes clear, these failures by the prosecution were not sporadic or isolated. Rather, they were of such a magnitude, and were so prevalent and pervasive as to constitute a pattern of conduct, that when all of the withheld evidence is viewed collectively, it is an inescapable conclusion that the Defendants' due process, confrontation and fair trial rights were violated . . . .").


the prosecutor. Thus, internal oversight sometimes can itself generate complicated moves and counter-moves.

6. CIPA, CIA Style

The CIA, almost without exception, does not allow raw cables to be turned over to defendants. Often these cables contain "cryptonyms" (code names for human intelligence sources). They also reveal CIA locations, personnel, and interactions with foreign governments, all of which are very sensitive and generally have only tangential relevance to a case. Under CIPA §4, an OGC lawyer works with prosecutors to propose "summaries" or "substitutions" that are acceptable to the Agency and eventually to the judge. Although redacted cables have been turned over to the defense, the recent trend at OGC is to lift relevant information from the cables onto separate pieces of paper. In some cases, prosecutors have convinced OGC to be more forthcoming in discovery with the promise that the prosecutors will limit the defendants' use of any classified information at trial.

At any stage of CIPA, OGC's practice is simpler if unclassified summaries can be approved. If not, the CIA insists that defense lawyers obtain security clearances as a condition of being able to review the classified discovery. Prosecutors with CIPA experience know all this, and at OGC's prodding they have convinced judges that the classified discovery should be shared only with cleared defense lawyers, not with the defendants themselves. The system does not take a chance by giving classified information to an alleged terrorist. Moussaoui is an example.

The disclosure of sensitive information in discovery does not by itself permit the defense to use that information at trial. Under CIPA §5, the defense must designate the classified information it intends to use at trial. Here, the usual pattern is for the defense to be too general in its designation, for the prosecution to insist on more specificity, and for the court to work out a compromise. Under §6, if the court determines that the designated information is needed at trial, the prosecution has another opportunity to propose summaries and substitutions.

Even when the §4 and §6 filters do not preclude the use of classified information at trial, the CIA may still allow the prosecution to proceed. Costs and benefits are weighed, and other techniques are considered for limiting disclosure. For example, the "silent witness" rule may be used to prevent an intelligence source from being publicly disclosed; all references in the courtroom and on the trial transcript may be to "Country A" or "Person A." Thus, only the judge, the parties, and the jury are told the actual names of the.

country and the person. Or, as happened in the Jose Padilla trial in Miami, a CIA officer may be allowed to testify in disguise.\textsuperscript{112}

CIPA is an expanding area of overlap between law enforcement and the intelligence community. All in all, the Justice Department’s interaction with OGC is usually positive. Prosecutors remind CIA officials that they sometimes need to defend their classifications before other executive agencies, judges, and defense lawyers. External checks and internal checks thus come together under CIPA.

7. Referrals and Opinions

Separate from civil cases and from the CIPA process, OGC lawyers interact with the Justice Department on criminal referrals, providing another opportunity for OGC oversight. The CIA’s Office of Inspector General, another internal guard at the CIA, also participates in referrals for criminal investigation, which are made pursuant to guidelines between the CIA and the Justice Department.

Referrals are sometimes made on mundane matters; others go to the core of the DO. A CIA employee may have submitted an inflated voucher for reimbursement of expenses for an official trip, leading to a prosecution for theft of government property or for false statements. Or an interrogation of an al Qaeda suspect may have gone beyond approved techniques, perhaps resulting in a suspect’s death.\textsuperscript{113} The CIA makes several referrals to the Justice Department in a typical month.

OGC also seeks legal opinions from the Justice Department.\textsuperscript{114} In this exchange, the General Counsel acts as a company lawyer to the CIA, and the Justice Department serves OGC as outside counsel of sorts.\textsuperscript{115} The CIA, if questioned about an activity, whether in court, on Capitol Hill, or by the public, can point to its comprehensive advice of counsel. This advice, on the interrogation of al Qaeda suspects or on other topics, may provide CIA officers with some protection from civil and criminal sanctions. In that sense, the August 2002 “torture” memorandum may still be useful to them, whatever

\textsuperscript{112} Jay Weaver, “Secret Agent” Testifies About Padilla Document, MIAMI HERALD, May 16, 2007, at 3A.

\textsuperscript{113} See Jane Mayer, A Deadly Interrogation, NEW YORKER, Nov. 14, 2005, at 44 (discussing whether CIA operative Mark Swanner would face legal consequences for the death of Manadel al-Jamadi, an Iraqi insurgent who died of “unnatural causes” while under interrogation by Swanner).

\textsuperscript{114} The United States government has acknowledged that OLC’s August 1, 2002, “torture” memorandum was prepared in response to a request from the CIA. See supra note 1.

\textsuperscript{115} A former OLC lawyer, Martin Lederman, has criticized the Bush administration for allowing parts of the Justice Department other than OLC to provide advice to the relevant agencies on U.S. counter-terrorism. See generally Walter Dellinger et al., Principles to Guide the Office of Legal Counsel, 81 IND. L.J. 1348, 1349 (2006) (“It is incumbent upon the Attorney General and the President to ensure that OLC’s advice is sought on important and close legal questions and that the advice given reflects the best executive branch traditions.”).
its analytical deficiencies. If these protections are deemed insufficient, the CIA may lobby for a Congressional fix. A case in point is the Military Commissions Act of 2006, which, following the Supreme Court's *Hamdan* decision, retroactively amended the War Crimes Act to restrict its coverage to a list of "grave breaches" of Common Article 3, rather than to all violations of Common Article 3.118

The General Counsel usually initiates requests for legal opinions from the Justice Department. She may want a second opinion on advice she has already given the Agency, or she may want somebody else's license on the line. Such CIA-DOJ interactions are tightly compartmented. At DOJ's Office of Legal Counsel, the group that handles the request may be limited to the lawyer who has the "CIA account," along with the chief and a deputy chief. The chief of OLC will, in turn, be inclined to brief the appropriate division chief, the Deputy Attorney General, and the Attorney General. If necessary, the Justice Department lawyers on the matter can be kept to a handful. The number of OGC lawyers will be similarly small: the General Counsel, the deputy General Counsel, the chief lawyer to the DO, and the one or two OGC lawyers assigned to the relevant division(s). Overall, not many guards are involved in legal opinions on sensitive topics.

**D. Post-Employment Duties**

Even after a CIA lawyer leaves OGC, she is not free from duties that relate to classified information. Potential watchdogs are taught to heel. Upon separation from the CIA, she signs another agreement, a reminder that she may not disclose anything classified. Her duty lasts for as long as she lives or for as long as the information stays classified. She is also reminded of the "pre-publication agreement" that she signed as a condition of her CIA employment. Before she publishes anything that relates to her CIA work, she must submit the manuscript to the Publications Review Board at CIA.119

The PRB does not require a former employee to notify the CIA if she is going to speak to the media or give a public speech without any written notes. It is at first surprising that the CIA trusts former employees to effectively protect classified information when speaking from memory, but does not trust

---

them when they put their thoughts on paper. There probably are at least two explanations for the disparity in procedures. First, it may be less practical, even impossible, for the CIA to police anticipated oral expression. Second, inadvertent oral disclosures may be less damaging than written ones. It is certainly easier for a foreign intelligence service to cull classified information from a written record, and no one from another intelligence service may even see a media appearance or hear a former employee’s remarks on a panel or to a group of students. Nonetheless, oral disclosures may be recorded and eventually be found in written form in a newspaper or on the Internet, blurring the apparently clear lines between oral and written expression. And where does “blogging” fit under the PRB rules?

Uncertainties about the content and application of PRB policy affect the free speech of former CIA lawyers. Because of PRB, for example, one professor decided not to offer his students a written syllabus in a national security course. Perhaps he was being too cautious — or too cute — but when he left the CIA, the head of the PRB had told him that even the name of his casebook had to be submitted. 120

The PRB claims that it goes no further than demanding the removal of classified items, and denies that it censors the writings of former employees who criticize the Agency. No matter the Board’s good intentions, the pre-publication review requirement may promote self-censorship or submissiveness. Former employees know their manuscripts will face some delay. The review of op-ed pieces takes days and weeks. Law review articles, including this one, take weeks and months. 121 And books take even longer. Whatever the form of her writing, the former employee is in a position of weakness. If she disagrees with the PRB about whether something is classified, she has internal recourse and may appeal to the courts. Such review, of course, takes time and money. Therefore, to avoid conflicts with PRB, a former employee is likely to err on the side of caution, pulling back on criticisms, pulling away from what may be classified areas. She heeds. Thus, I acceded to the PRB request that minor deletions be made in this article. Rather than challenge what I considered an inaccurate view of what is classified, I was relieved that the suggestions were not more substantial.

Valerie Plame, the former CIA officer at the center of the Scooter Libby case, is one person who did not accept the PRB’s redactions. Backed by her publisher, Simon & Schuster, Plame took the CIA to court in the Southern District of New York in an effort to publish her memoirs without redactions. 122

120. Apparently NATIONAL SECURITY LAW (4th ed. 2007) by Stephen Dycus and his colleagues passes CIA muster.

121. I submitted a draft of this article to the PRB in mid-July of 2006. I did not receive a response, proposing minor deletions, until the end of October 2006.

yet this suit may have been meant to garner publicity as much as it was to overturn the PRB’s decision.

For Please and many others, the heavy cloak of CIA secrecy prevents those who know the most about the Agency from describing abuses. Very few veterans from OGC have been foolish enough or brave enough (or both) to speak out about the Agency. Two former general counsels, Anthony Lapham and Jeff Smith, have been quoted. And a former assistant general counsel has spoken up.

In dealing with the Agency, the guardian is in a weak position. She may resign from OGC on principle. But even after she resigns there are severe limits on what she may say. She may allege that the CIA is way off course. The CIA is shameful, she may add. When pressed to back up her allegations, however, she may not refer to specifics. She may believe that secret prisons violate U.S. and international law, but her bosses, including the General Counsel, may disagree. They have the two-edged weapon of Commander-in-Chief powers and the executive prerogative to decide what remains classified. When she is inside the Agency, they can shut her out through tight compartments of information. When she is outside the Agency, they can shut her up through the PRB.

If a former employee defies the PRB by not submitting a manuscript for review or by not incorporating the PRB’s suggested changes, she is exposed. She may argue that the manuscript does not fall within the scope of her prior

123. Anthony Lewis, Abroad at Home: The Greater Threat, N.Y. TIMES, Feb. 21, 1985, at A23, ("[A] former C.I.A. general counsel, Anthony Lapham, said in 1979..." We have had in this country for the last 60 years an absolutely unprecedented crime wave, because surely there have been thousands upon thousands of unauthorized disclosures of classified information..."’); Tim Weiner, The Mideast Talks: Cloaks and Daggers, The U.S. Intelligence Chief Steps Up to the Plate, N.Y. TIMES, Oct. 23, 1998, at A12 (”C.I.A.’s relationships with the intelligence services in both countries allow it to bridge gaps otherwise unbridgeable,’ said Jeffrey Smith, who as the general counsel of the agency worked with Mr. Tenet on his mediation efforts in 1996.”); see also Jeffrey H. Smith, Op-Ed., Secret Lives, Honest Spies, N.Y. TIMES, Nov. 27, 1996, at A25.

124. Peter Baker & Michael Abramowitz, A Governing Philosophy Rebuffed, WASH. POST, June 30, 2006, at A1 (“Rather than push so many extreme arguments about the president’s commander-in-chief powers, the Bush administration would have been better served to work something out with Congress sooner than later — I mean 2002, rather than 2006,” said A. John Radcan, a former C.I.A. lawyer who now teaches at William Mitchell College of Law.”); Douglas Jehl, Report Warned C.I.A. on Tactics in Interrogation, N.Y. TIMES, Nov. 9, 2005, at A1 (“The ambiguity in the law must cause nightmares for intelligence officers who are engaged in aggressive interrogations of Al Qaeda suspects and other terrorism suspects,” said John Radcan, a former assistant general counsel at the agency who left in 2004.”); Dana Priest, Covert C.I.A. Program Withstands New Furore; Anti-Terror Effort Continues To Grow, WASH. POST, Dec. 30, 2005, at A1 (“In the past, presidents set up buffers to distance themselves from covert action,” said A. John Radcan, assistant general counsel at the CIA from 2002 to 2004.”); Scott Shane, Seeking an Exit Strategy for Guantanamo, N.Y. TIMES, June 18, 2006, §4 (Week in Review), at 1 (”Mr. Radcan, the former C.I.A. lawyer, offers a more measured critique... He says the secret detainees held abroad are a more serious constitutional concern than the Guantanamo inmates, because they have no access to any legal process.”).
work at the Agency, but that argument only goes so far. If the former employee does not go through PRB and if she earns profits from the manuscript, the CIA can take those profits through a constructive trust, as noted in the Snepp case.\textsuperscript{125} In such situations, even the lawyer who seeks to be a watchdog is tamed.

I am told that Bob Baer, a former CIA case officer, did not make changes the PRB requested in his book See No Evil.\textsuperscript{126} If he published the book with passages the PRB had designated for redaction, he took a risk. And the risk may have paid off. The Hollywood movie Syriana was based, in part, on Baer’s book.\textsuperscript{127} The movie sold many tickets, and with Hollywood on board it is safe to conclude that Baer made some money.\textsuperscript{128} Under the Snepp doctrine, the CIA may still covet those profits.

Apart from the possible loss of profits, a former employee who defies PRB may face serious difficulties in obtaining a security clearance if she decides to return to government service. Baer might well accept that as the price of his defiance. Perhaps an even greater concern for a defiant former employee is the threat of criminal prosecution. Baer, who served the CIA in Lebanon, Iraq, and other tough places, can probably handle the anxiety. But former CIA lawyers may not be so tough. While the Justice Department has not been keen on bringing prosecutions against CIA employees for leaks, that reluctance can change in an instant. The former employee can, like Frank Snepp, be made an example by the Agency. Accordingly, the CIA uses the possibility of criminal or civil proceedings to control its former employees, transforming them from potential watchdogs into lapdogs.

Out of self-interest, former employees closely follow the back and forth of the PRB pendulum with each new Director. The Porter Goss regime turned.

\textsuperscript{125} Snepp v. United States, 444 U.S. 307 (1980) (per curiam) (imposing a constructive trust on profits from a book that a former CIA case officer wrote about what he considered the CIA’s shameful performance at the end of the Vietnam War, not because the book contained any classified information or secrets, but because it was not submitted to the CIA for pre-publication review as the author had agreed by signing an agreement and by entering into a relationship of trust with the Agency).

\textsuperscript{126} Baer, who had over 20 years of experience at the CIA, is an outspoken critic of the Agency.

\textsuperscript{127} George Clooney won an Academy Award for best supporting actor for playing the Bob Baer character. See David M. Halbfinger & David Carr, “\textit{Crash” Walks Away with the Top Prize at the Oscars}, N.Y. \textit{Times}, Mar. 6, 2006, at E1. In a touch of irony, Bob Baer himself has a cameo role as an unctuous employee of the CIA’s Office of Security. The Baer character greets the Clooney character in a hospital after a Hezbollah crazy has pulled out Clooney’s fingernails. In the movie, the Office of Security, true to its real-life role, is more concerned about any secrets that may have been divulged than about Clooney’s well-being.

\textsuperscript{128} When I invited Baer to speak at the National Security Forum at William Mitchell College of Law, his agent at Creative Artists Agency informed me that his usual speaking fee is $15,000. Baer has not yet appeared at the Forum.
out to be tougher than the George Tenet regime.\textsuperscript{129} For the moment, it is too soon to read Michael Hayden, the new DCIA.

V. ROTATION AND ADVANCEMENT

The prize for an OGC lawyer is being assigned to the Directorate of Operations,\textsuperscript{130} the place where she becomes the ultimate company lawyer. With an eye on the DO prize, she toils as a junior lawyer on FOIA requests and on other less than glamorous assignments.

A. The DO Versus the Rest

Differences exist at the CIA among the analytical wing (the Directorate of Intelligence), the technical wing (the Directorate of Science and Technology), and the support wing (the Directorate of Support). There are also integrated centers that transcend separate directorates: the Counterterrorism Center and the Counter-Intelligence Center. But the biggest split in the CIA is between the DO and everybody else. The DO is a special place, a dominant culture at the Agency. To highlight these differences, I focus on the DO against the backdrop of the DI. The DI, in my comparison, represents all those parts of the CIA that are outside the big, bad DO.

1. Different Goals

Although the line between collection and analysis is not always clear, the separation between the DO and the DI reflects a common split at intelligence services. The DO collects foreign intelligence, takes covert action, and conducts counter-intelligence. The DI reviews what the intelligence community has collected (human source reports, intercepts, satellite photographs, open-source reports, and many other items) and converts the raw data into written and oral reports for policy makers.

The highest prize for the DO is recruiting a foreign country's head of state as a source. Next best is the head of that country's intelligence service. From the early days of the CIA, the highest product for the DI was the President's

\footnotesize{\textsuperscript{129} See Douglas Jehl, \textit{New C.I.A. Chief Tells Workers To Back Administration Policies}, \textsc{N.Y. Times}, Nov. 17, 2004, at A1 (reporting the discovery of a memorandum written by Goss that outlined Goss's expectations of CIA employees, which "appeared to be a swipe against an agency decision by George J. Tenet . . . to permit a senior analyst at the agency, Michael Scheuer, to write a book and grant interviews that were critical of the Bush administration's policies on terrorism"); Porter Goss, Op-Ed., \textit{Loose Lips Sink Ships}, \textsc{N.Y. Times}, Feb. 10, 2006, at A25 (asserting that "those who choose to bypass the law and go straight to the press are not noble, honorable or patriotic. Nor are they whistleblowers. Instead they are committing a criminal act that potentially places American lives at risk. It is unconscionable to compromise national security information and then seek protection as a whistleblower to forestall punishment.").}

\footnotesize{\textsuperscript{130} See supra note 15.}
Daily Brief, a classified digest of trends and developments. Now the Office of the Director of National Intelligence has taken over that production, and the DNI, not the DCIA, now meets with the President on a daily basis. Next best for the DI is its leading role in preparing National Intelligence Estimates, the inter-agency conclusions on major national security issues. The public learned about NIEs, their virtues and flaws, in the run-up to the 2003 invasion of Iraq.

2. Different Styles

On the CIA campus, the DO personnel are the jocks and the DI personnel are the nerds. The people in these two directorates keep their distance, their views of one another shifting between respect and disdain. The DO officers I met, whether in a restaurant or in the office, were always on, always assessing, always working the situation. The world was a big operation for them. They made passes at waiters and waitresses for the fun and practice. The DI officers, by contrast, were more likely to separate their work from their socializing. With them, it seemed possible to have a conversation that did not have an ulterior motive. They behaved.

The work in the two directorates also differs. The DO officer convinces people from other countries to commit espionage. The recruitment cycle from assessment to development to pitching to handling is complex, but the goal is simple: convince a foreigner to turn over his country's secrets or to betray his group. In the past, the DO officer ran arms to rebel groups, planted stories in the foreign media, and passed money to foreign political parties. He has been on guard against our enemies in the dark alleys, on the look-out for sources and agents in caves and back streets. The Special Activities Division within the DO handles paramilitary activities and other aspects of covert action. To the extent that the CIA is involved in Predator strikes on suspected terrorists, SAD probably has a role.

The DO officer, whether in SAD or in other divisions, must be an extrovert or at least be able to draw upon the active side of his personality. More than anyone else at CIA, the DO officer is the guard in need of a guardian. He works the farthest from headquarters. His potential excesses,
such as stealing from an asset’s cash payment, sleeping with an agent, or killing a source, are perhaps the most costly.

The DI officer, cut from a different cloth, is like a university professor. He solves puzzles by extrapolating from less than a full box of pieces. He takes the bits of what the intelligence community has collected and fits them into the so-called intelligence mosaic. His mistakes, such as sloppy analysis and mirroring American assumptions onto our adversaries, are costly, too; they may lead to unjustified wars and to surprise attacks against us. But other people, other analysts at the CIA and elsewhere, review his work. Because his excesses are not immediately fraught with death and bodily injury, he is perhaps less in need of a guardian.

3. Different Education

In the early days of the CIA, Ivy League universities provided a high percentage of the recruits who became case officers and analysts. Spying, no matter the particular function, was for gentlemen. Things have changed. Today, the typical CIA recruit is more likely to have a degree from the University of Michigan than from Princeton.

Not everything has changed, however. Today, as in the past, the DI has a higher percentage of officers with advanced degrees than the DO. Many analysts are recruited from masters and doctorate programs in international affairs and area studies. While it is next to impossible to become a case officer without a college degree, the DO does not emphasize academic merit as much as the DI does.

In the early days of the CIA, many DO types had paramilitary experience from their World War II days in the Office of Strategic Services. DO people are jumpers, DI people are not. The DO people, as much as they look down on FBI agents as cops, come across as G-men. George Smiley from John Le Carré’s fiction is the British version of a calculating DO man. DI people, by their dress and by their hairstyles, would be comfortable at the Brookings Institution. Tacked onto the walls of their cubicles are charts, cards, and photographs. Jack Ryan from the Tom Clancy novels is a DI man.

4. Different Training

All CIA employees receive briefings. Assigned all over the Agency are officers from the Office of Security who remind the various sections and directorates about the proper handling of secrets. They all have PowerPoints and videos, but additional training in the DO is quite different from that in the DI.

DO people, destined to serve in the field, receive months of basic training at a facility called the Farm. Among many things, they learn about secret communications, detecting surveillance, and parachuting to the ground from an airplane. Later in their careers, or for special assignments, they receive additional training. They learn to do.
Unlike DI officers, DO officers are unlikely to receive training that requires wading through swamps. Instead, DI officers are more likely to study Immanuel Kant on how categories influence the phenomenology of data. They learn to synthesize.

5. Different Digs

The locations of work for DO and DI differ. Although the DI assigns some officers to locations away from headquarters, most analysts spend comfortable careers in the Washington area. DO officers, on the other hand, fill the bulk of CIA stations overseas. Accordingly, the field person is most often somebody from the DO. As soon as he finishes training at the Farm, the DO officer is anxious to join the action overseas. Through experiences in the field, the heads of DO components gain their posts and the respect of their peers. That is where the legends are made.

Back at headquarters, the daily meeting of the DDO with the heads of components is called the meeting of intelligence barons. This meeting, filled with spymasters, may be even more prestigious than the Director's morning meeting. The Director's meeting includes political appointees, such as the General Counsel and the Executive Director. The barons' meeting includes professionals, mostly men and women who have made things happen in the field; the General Counsel, an outsider, usually does not attend.

The barons do not fully respect people different from them, and barons look down on other barons who are relatively lighter on field experience. For example, when James Pavitt was DDO under George Tenet, the barons could barely hide their disdain for him. When Michael Hayden was named DClA, Steve Kappes, field man extraordinaire, was brought back to CIA as DDCIA to reassure the DO troops that the White House still respected their mastery in human source operations.134 Another nod to the DO was John Rizzo's nomination to be General Counsel.

6. Different Covers

Officers from both the DI and the DO use cover, not revealing their CIA affiliation in public. Some use official cover, a claim that they work for another United States agency. Some use non-official cover, a claim that they work for a non-governmental employer. Those in this second group, "illegals," do not benefit from diplomatic immunity. If a foreign intelligence service catches them engaged in espionage, they can be prosecuted in that country.

Because DO officers operate in the field, often in hostile environments, a higher percentage of DO officers than DI officers use cover. It is difficult, if

not impossible, for CIA personnel to be admitted to foreign jurisdictions if
they tell immigration authorities that they work for the CIA. “Hello, I am here
to recruit spies,” is not a good opening line. Even in those countries where the
foreign intelligence services know what our DO officers truly do, the cover
stories make it easier for host governments to deny (or to justify) the CIA
presence there. Imagine the costs otherwise to leaders in the Middle East for
cooperating with the CIA.

Some analysts may benefit from cover even though they do not recruit and
run human sources. Valerie Plame may be an example. As a part of her
duties, an analyst may attend conferences and seminars and may surf the
Internet. An open CIA affiliation could make it difficult for her to be invited
to conferences in some countries or to be allowed access to some websites.
Cover is part of the solution for her.

An improper rolling back of cover can have grave consequences for both
DO and DI people. The improper roll-back puts the officer and everyone with
whom the officer has interacted in danger. Now that al Qaeda has replaced the
Soviet Union as the main enemy, the threats to CIA officers are even greater.

If the counter-intelligence branch at another country’s service determines
that an officer is actually CIA or suspects a CIA connection, it will walk back
that officer’s interactions. To do so, the other service will review surveillance
logs and other records. In the review, what might once have seemed
innocuous may be seen in a different light. A person from that foreign service
may find it more difficult to justify a past meeting with an American who is
confirmed as a CIA officer. Spies may be exposed, networks rolled up.

The general split between the DI and the DO at the CIA replicates itself
on a smaller scale in the Office of General Counsel. OGC does assign lawyers
to the DI, but those people do not strut their stuff. The lines are clear at CIA.
There are those who work for the DO — and there is the rest of the office. The
DO lawyers adopt the DO’s disdain for the rest of the Agency. They are the
insiders on the move. With the importance that comes from busyness, they
check their watches more often than the plodders do.

B. Selection into the Club

The chief DO lawyer, someone with many years of Agency service, has
great influence in deciding who is deployed from the OGC ranks as a lawyer
for the DO. The chief DO lawyer makes recommendations to the OGC front
office (the General Counsel’s suite on the seventh floor) about assignments
into various divisions of the DO. Thus, the chief DO lawyer, who is not
located in the OGC front office, stands in the reporting line between the
General Counsel and the “component” lawyers, whether in Africa Division or
Latin America Division or elsewhere.

It is almost unheard of for a lawyer in OGC, no matter how many years
of experience the attorney has elsewhere, and whether hired through the
honors program or the lateral program, to be assigned straight into the DO
upon joining the CIA. She must pay her dues and be assessed by her peers in
other parts of OGC, where she is tamed. Further, she must learn the office’s line on what separates properly advising on the law from improperly intruding into policy discussions.

Except during times of scandal or during the reign of an aggressive General Counsel, a lawyer who views her role as “providing adult supervision” will not be sent into the DO. Beyond technical competence, the DO prefers that its lawyers have bought into its culture. DO lawyers, whether by OGC’s plan or by inertia, learn to accept the Directorate’s special mores.

In selecting lawyers for DO service, OGC consults the front office in the relevant division. Such consultation gives the DO an opportunity to scout its lawyers. The scouting is done by case officers who, after all, are reasonably adept at gathering intelligence. Only rarely will OGC impose a lawyer against the will of a division. The DO, aware of this, will not easily accept a lawyer who, based on a division’s assessment, is going to be a problem. Of course, one person’s “problem” may be another person’s “oversight.”

Even when a CIA lawyer makes it into the DO, she will most likely be the junior person in a component that has more than one lawyer (for example, the Near East Division). She benefits from a senior lawyer’s mentoring and training, but at least one other person, either the chief DO lawyer or the senior lawyer in the division, watches for signals that she is likely to create problems for DO officers rather than resolve them. It is uncommon, however, for CIA lawyers to be transferred out of DO service—once in the club, always in the club.

A DO lawyer needs to have a close relationship with the division in which she serves. She will not be very useful, whether providing oversight or facilitating deals, if the division’s front office and other officers do not trust her. She will be decoration, the tamest of lapdogs.135 There are just too many special channels of communication for her to make complete sense of the job on her own. The DO lawyer, to be most effective, needs to tap into what is known as “RUMINT,” the hallway talk, the phone calls, and the discussions in the cafeteria. Without the intelligence of rumors—not to be confused with signals intelligence (SIGINT)—the DO lawyer would drown in the ordinary channels of information, the cables and emails, that fill her office. For special access, she cozes up to DO officers. This is another way watchdogs are tamed.

C. Inevitable Conflicts

Throughout the Agency, supervisors review the performance of their officers. The most important reviews are done annually in writing. In my day, these reviews were called fitness reports. As at many academic

---

135. One lawyer assigned to the European Division worked for weeks before anyone other than a secretary would talk to him.
institutions, the CIA inflates its grades. Faint praise is feared, and officers look for hidden messages anytime a superlative is not used.

Many years ago, when OGC first decided to deploy lawyers to the DO, an important issue was who would write the lawyers' fitness reports, OGC supervisors or DO managers. A reasonable argument can be made for either reporting channel. Because DO managers regularly work with their lawyers, they have the most data. Because the lawyers need independence in providing what may be unpopular advice, however, and because lawyers appreciate the quality of legal practice better than lay persons, OGC supervisors should be involved. A hybrid solution has OGC supervisors write the reports with some input from DO managers. The chief DO lawyer then meets with each component lawyer to go over his report and to have her sign it, a resolution that reflects a rough compromise between the OGC lawyer's role of outside oversight and that of company lawyer. Thus, the relative roles for OGC and the DO in preparing fitness reports may mark the boundary between oversight and facilitation. In any case, the more DO managers participate, presumably, the less potential there is for oversight.

Some DO officers resent the privileges enjoyed by OGC personnel. Because lawyers hold advanced degrees, they start much higher on the government pay scale, and a rank of GS-15 can be reached quickly. For case officers, the GS-15 rank is the prize at the end of a long career. Further, OGC has a disproportionately high representation in the ranks beyond the GS scale, the senior intelligence service (SIS). The rank of SIS thus merits more respect in the DO than in OGC, where it is less unusual.

Lawyers in the DO have separate offices. Those quiet offices go with the deep thinking they are supposed to do. It is their right. In the rest of OGC, only the most junior lawyers suffer the indignity of having to double up in offices, and that indignity lasts at most a few months. At headquarters in the DO and the DI, except for the front offices in the two directorates, most CIA officers work in cubicles and shared spaces. They are out on the floor. For a case officer or an analyst, an office is a privilege, a sign that the employee has moved into managerial duties.

Other substantial lines divide lawyers from other CIA personnel. If a DO officer falls under the Inspector General's suspicion or, worse, the Justice Department's, the most the DO lawyer can do is advise the officer that she does not represent his personal interests. She may, as a matter of first principles, give him unsolicited advice to retain personal counsel.

Having worked in close quarters with the DO officer, the DO lawyer will be tempted to give free advice. When she acts on temptation, the DO lawyer best not leave a paper trail. Moreover, she must consider whether she is willing to cover up the communication if the Inspector General or the Justice Department asks her about it at a later date. Even if she trusts the DO officer, even if she scripts with him, she cannot be sure that her story will correspond with his when they are questioned separately under oath. Acting on such temptations thus takes the DO lawyer into uncomfortable territory that
includes possible false statements and possible obstruction of justice. The safest course for her is to wipe her hands clean of the DO officer.

If the Inspector General or the Justice Department is investigating a DO officer for wrongdoing on an operation, the investigators may seek to minimize OGC's role. But even if OGC refuses individual advice to the DO officer under investigation, OGC still may be involved. For example, if the DO officer retains counsel on his own, his lawyer will need to have a security clearance. OGC's Litigation Division usually has a role in checking such clearances and in processing the applications for them. Therefore, in order to limit OGC's involvement the Inspector General's Office or DOJ will need either to take over those duties for the investigation or to coordinate with OGC on clearances. Otherwise, the checking of security clearances and the application for clearances will give private counsel a chance to ask OGC about the course of the IG/DOJ investigation and will give OGC a chance to volunteer such details. It is contrary to common sense to suggest that such interactions will never result in some inadvertent seepage of information. Some OGC lawyers, especially those loyal to friends in the DO, may even talk out of school. Thus, watchdogs may be converted into lapdogs for their DO masters.

The relationship between the General Counsel and the Inspector General at CIA is crucial to effective oversight. Faced with a criminal investigation of CIA officers, the General Counsel may argue to the Inspector General that an OGC lawyer needs to attend interviews between the IG/DOJ and the DO officers. The General Counsel may say this is necessary not to represent the person under investigation but to protect the institution. The General Counsel may argue that OGC needs to stay current on the case to advise the DO's management about whether DO officers need to be reassigned or put on administrative leave. The IG/DOJ may counter that staying current on the investigation does not require attendance at the interviews; IG/DOJ can let OGC know.

Sometimes the General Counsel and the Inspector General reach accommodations on such issues. If they are unable to find a compromise, legal authorities in the form of statutes, regulations, and internal guidance are thin. To resolve their disputes, they may appeal to their mutual boss: the DCIA. The DCIA will be able to direct OGC where to stand between oversight and facilitation.

136. An ethical issue beyond the scope of this article is the propriety of joint Inspector General-Justice Department investigations. A CIA employee cannot refuse an Inspector General interview without administrative consequences. On the other hand, unless she is given immunity, a CIA employee preserves her Fifth Amendment privilege against self-incrimination in criminal investigations. Accordingly, a CIA employee who is told by a Justice Department prosecutor that an interview is "completely voluntary" may focus less on those words than on the presence in the room of an investigator from the Inspector General's office.

137. I know OGC lawyers who helped DO officers select private counsel. I know one senior OGC lawyer who convinced private counsel to put off charging clients until the Agency could determine whether official funds could be used to pay for the representation.
Even if the Inspector General keeps OGC lawyers out of the interviews, the IG/DOJ may need OGC’s assistance. Current officers are as available to the Inspector General as they are to the General Counsel, but retired and former officers are a different matter. CIA personnel are accustomed to making OGC their first stop for inquiries about what they are allowed to say in legal proceedings. Before an officer retires or leaves the CIA, he receives a briefing on how much, if anything, of his Agency activities he is allowed to discuss. As a part of the officer’s ongoing obligations, he is told that he must contact OGC any time he is about to be drawn into litigation.138 The scope of this obligation is broad enough to cover testifying in a child custody dispute, contesting a traffic ticket, or being questioned by the IG/DOJ. A well-briefed officer will not say anything until he obtains guidance and authorization from OGC. Even if the Inspector General assures the former officer that he can speak to the IG without contacting OGC, that officer may insist on confirming that the Inspector General has the authority to step in for OGC. Such insistence may, of course, be sincere or it may be a stalling tactic. In either case, OGC may play a role in arranging for the interview with the Inspector General.

These kinds of ethical issues exist in Agency practice but are rarely discussed in scholarship. In practice, at least one General Counsel has pulled aside at least one OGC lawyer in an effort to shape his loyalties. Remember, Scott Muller told me, when Justice comes after “our” officers, they are coming after all of “us.” The General Counsel wanted to make sure that the Agency took care of its people. As a new boss, he was proving himself. Be that as it may, the public should expect such lines from the Godfather, not from the CIA’s General Counsel. Alas, the General Counsel’s performance sometimes does not live up to our expectations of a balanced and better breed.

VI. SYNTHESIS

A. Various Mixes

It is not feasible for the CIA’s General Counsel to be a total watchdog. If she yelps, barks, or whines too much, her political masters at the CIA will put her out in the yard. But she should not be a total lapdog, either. She should

138. “Whenever a demand for production is made upon an employee, the employee shall immediately notify the Litigation Division, Office of General Counsel, Central Intelligence Agency . . . which shall follow the procedures set forth in this section.” 32 C.F.R. §1905.4(a) (2006). “If oral or written testimony is sought by a demand in a case or matter in which the CIA is not a party, a reasonably detailed description of the testimony sought, in the form of an affidavit or, if that is not feasible, a written statement, by the party seeking the testimony or by the party’s attorney must be furnished to the CIA Office of General Counsel.” Id. §1905.4(d).

“Demand means any subpoena, order, or other legal summons (except garnishment orders) that is issued by a federal, state, or local governmental entity of competent jurisdiction with the authority to require a response on a particular matter, or a request for appearance of an individual where a demand could issue.” Id. §1905.2(b).
serve as more than an ornament, totally responsive to the whims of her masters. The General Counsel should be a mixed breed — somewhere between a watchdog and a lapdog, somewhere between strict overseer and adamant facilitator.

Just what mix of watchdog and lapdog the General Counsel is depends to a large extent on the will of the political leadership at the CIA and the White House and, to a lesser extent, on the will of Congress, the media, and the people. On this continuum, the Carter White House preferred watchdogs. It was disgusted by CIA excesses revealed by the Church Committee, including assassination plots, human rights abuses, and the surveillance of U.S. citizens. President Carter, emphasizing the importance of human rights in American foreign policy, appointed Stansfield Turner as DCl. Turner was a vigilant director whose first order of business was to trim the ranks of the DO. An expanded Office of General Counsel was part of this new vigilance, and some flexibility in operations was traded for more enforcement of the law. It was a time for watchdogs.

After the hostage crisis in Iran and the Soviet invasion of Afghanistan, U.S. foreign policy swung to the other end of the continuum. The Reagan White House, inspired by conservative think tanks, sought to correct what it perceived as President Carter’s fecklessness. The intelligence community was used by President Reagan to reassert U.S. power. Upon election, President Reagan appointed his campaign manager, William Casey, a trusted insider, as DCl. Casey, until his death in office, led an aggressive CIA campaign against the “Evil Empire” on many continents, supplying the Mujahadin against the Soviets in Afghanistan and helping the Contras challenge the Sandinistas in Nicaragua.

In the new environment after 1980, the Office of General Counsel at the CIA was called on to enable the company, and some enforcement of the law was traded for operational flexibility. It was a time for lapdogs. If policymakers forgot a written finding for a covert action, an enabling General Counsel facilitated them with a retroactive one.139 OGC, hand in hand with the National Security Council, was eager to accommodate the President. Some CIA officers were indicted for their role in the Iran-Contra affair, and only presidential pardons140 and CIPA technicalities141 saved them from convictions.

Depending on our political leaders and on the perceived external threat, the pendulum will continue to swing between the Carter and the Reagan

139. Stanley Sporkin, Casey’s friend, was CIA General Counsel at the time.
140. The first President Bush pardoned former DDO Clair George and former Division Chief Duane Claridge. David Johnston, The Pardons; Bush Pardons 6 in Iran Affair, Aborting a Weinberger Trial, N.Y. TIMES, Dec. 25, 1992, at Al. George was convicted on false statement and perjury charges. Id. Claridge was awaiting trial on similar charges. Id.
approaches to intelligence activities. The activities of spymasters, operating on the dark side, will oscillate between retrenchment and reassertion. Even within a particular administration, a General Counsel’s behavior may shift across the continuum.

In the range between oversight and facilitation, General Counsels will have different default modes. McNamara’s was not the same as Muller’s. Muller’s was not the same as Rizzo’s. General Counsels will not, of course, decide all matters from their default positions. From decision to decision, each one shifts toward either watchdog or lapdog. So much depends on the situation. In one situation the General Counsel’s advice to the DCIA about congressional testimony may be strict. In light of possible perjury and false statement charges, she may insist that the truth be told in response to specific questions. In another case, the same General Counsel may be less strict. For purposes of congressional notification, she may be less categorical about what activities fall within the statutory definitions of covert action and significant anticipated intelligence activities. In making such fine distinctions, she might even distinguish between committed acts and omitted acts.

B. A Delicate Scenario

Even the most vigilant guards cannot prevent all misconduct, a fact that stands true in our day as much as it did in Juvenal’s. Oversight of an intelligence agency, whether internal or external, is limited. Lawyers cannot prevent or ferret out all wrongdoing. Some spymasters who break the law will not be caught. Some policy makers who push activities beyond established lines will not be punished. Juvenal’s question about who will guard the guard may, after all, simply be a rhetorical statement about human imperfection. Many scenarios can be constructed involving spymasters who escape criticism, policy makers who cross established lines, or lawyers who are cut out of the action.

Imagine that a foreign country captures a high-level al Qaeda operative. Only a few people in that country’s security and intelligence services know about the capture. During a state visit to Washington, the country’s prime minister asks for a one-on-one meeting with the President of the United States. The President agrees, and the two men meet in the Oval Office without note-takers and without any recording. When the prime minister tells the President about the capture, the President nods his interest. The prime minister, trusting the President not to publicize the capture, offers to make the captive available to American interrogators. The two heads of state agree that direct involvement in an interrogation is sometimes better than passing questions through intermediaries.

The President accepts the prime minister's offer. The prime minister suggests that the day-to-day interaction should be between the DCIA and the head of the foreign country's intelligence service. The prime minister and the President shake hands. Then, the President opens a door to let their advisors into the Oval Office. All they say is that they had a good chat.

The next day the President contacts the DCIA. They also have a one-on-one meeting in the Oval Office – no notes, no recording. The President explains that he accepted the prime minister's offer to have CIA officers question the captive directly in that foreign country. The DCIA smiles. "That is great news, Mr. President." The President instructs the DCIA that only those with an absolute need to know should be included in the project.

The DCIA asks whether they need a finding for covert action. The President writes something down for the DCIA. Then he looks the DCIA in the eye. "I have the constitutional authority as Commander in Chief to keep this to ourselves," the President declares. "Later, we'll decide what we tell the Hill."

The DCIA asks the President whether the CIA's General Counsel should be included. The President responds, indirectly, that he has already received sufficient legal advice from the Justice Department and the White House Counsel. The DCIA, pleased to be back in direct contact with the President, accepts the response. The DCIA has one additional question, though. "How tough can we be on him?" Wincing, the President shows his displeasure. "Stay within the law," he says. "But do what needs to be done."

Back at CIA headquarters, the DCIA calls the Deputy Director of Operations on a secure phone. The DCIA and the DDO meet in the Director's suite. They do not take notes, do not record their conversation. Neither the Deputy Director of the CIA nor the Executive Director nor the General Counsel is informed. The DCIA tells the DDO to select two senior officers to handle the interrogation. The officers are to report only to the DDO. The DCIA is to be the only point of contact with the head of the foreign intelligence service. The DDO agrees to the strict compartments. He identifies two other issues and, in the course of their conversation, comes up with two solutions.

First, to prepare for the interrogation, the interrogators will need to search the Agency's databases for information about the suspect. To leave the smallest trail, the DDO will run those searches himself. Second, if the captive provides information to the aggressive interrogators, they will need a means of informing the President and the rest of the intelligence community about the take. The DCIA and the DDO do not want to reveal that U.S. interrogators played a part in extracting this information. To accommodate their wishes, the extracted information will be shared with the foreign intelligence service. The foreign intelligence service can then provide the information back to the CIA through a restricted channel. The liaison service will appear to be the original source.

The DCIA and DDO, both accustomed to various means of protecting their sources, do not consider this end-around to be at all significant. Rather,
they are focused on the rare opportunity to interrogate a high-level al Qaeda operative.

After the meeting, the DDO selects two officers for the interrogation. They are fluent in Arabic, the captive's native language. They are senior managers in the DO with extensive field experience. Because they have traveled to the foreign country several times in the past, their travel this time will not raise too many eyebrows. They ask the DDO whether they should inform the CIA chief of station in the country about their operation. The DDO and his two officers agree that even if they did not tell the chief of station, he would find out from the liaison service or from his own sources in the country. So they agree to inform him with vehement instructions that he not tell anyone else. "Strict need to know," the DDO reminds them.

The two officers have the CIA's travel office arrange their flights to the foreign country. There, during an aggressive interrogation, including sleep deprivation and bombarding the suspect with lights and music, they extract very useful information from him. The information comes to the CIA and then circulates within the U.S. intelligence community. A few OGC lawyers read the cables, but they have no idea what went on behind the interrogation.

As a result, the operation has been run with the knowledge of six Americans: the President, the DCIA, the DDO, two case officers, and a chief of station. Congressional notification is put off into the indeterminate future. To the extent that this operation raises issues of law, such as reporting to the oversight committees and the President's power to order torture, those issues may not be addressed by lawyers in the intelligence community. They remain the fantasies (or the nightmares) of imaginative law school professors. Lawyers, wherever they are located, and however much they strive to attain a balance, can only do so much.

C. Final Notes

Throughout American history, Presidents have been tempted by Commander-in-Chief powers and by executive authority to keep information classified. Secretly, they have supported coups and killings away from the traditional battlefield. Whether in Chile or in Laos, spymasters have usually done their Presidents' bidding on the dark side. If Presidents have insisted on the utmost secrecy, spymasters have accommodated them, cutting out Vice Presidents, cabinet secretaries, and ambassadors. The spymasters have also cut out other intelligence officers, friends, whom they or the President determined did not have a need to know. The harsh reality in intelligence activities is that cutting out a few lawyers is just as easy, even easier.

143. Exceptions exist. For example, when DCI Richard Helms did not take the White House's suggestion to invoke "national security" reasons in order to steer the FBI off the Watergate investigation, he was demoted to American ambassador to Iran.
In basic terms, the Presidents’ varying approaches to the rule of law parallel those of the General Counsels at the CIA. Some Presidents, like President Carter, may have strictly adhered to the letter of the law on intelligence activities. Some Presidents, like President Reagan, may have strayed. Some CIA General Counsels have followed their President’s course; some have strayed. Even when Presidents and General Counsels share similar courses, they are not always in lock-step, because too many layers of executive authority – White House Counsel, the National Security Adviser, the DCIA, and other staffers – often stand between them. Yet the President and the General Counsel have an effect on each other, even if that effect is indirect and not easily measured.

To understand how lawyers affect intelligence agencies, one can identify a General Counsel’s usual position between watchdog and lapdog, then observe shifts from that position on particular decisions, such as aggressive interrogation, the destruction of interrogation tapes, and referrals to the Justice Department for criminal investigation. The journalist with inside sources or the lawyer working on the inside can be more effective in making these observations than the typical scholar. Even so, no matter how much information is gathered or by whom, an analysis of CIA lawyers cannot penetrate too far beneath the surface. That is not to say that this analysis is worthless. It is merely to admit, in the humblest of terms, the difficulty in penetrating any reality, especially a classified reality.

The CIA’s Office of General Counsel, when it lives up to its promise, serves as one guard over the activities of the CIA. The lawyers there are not perfect, but as watchdogs, lapdogs, and mutts they answer Juvenal’s famous call for some sort of guard over the guardians.
STATEMENT

OF

LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

“COUNTERING TERRORIST FINANCING: PROGRESS AND PRIORITIES”

PRESENTED

SEPTEMBER 21, 2011
Statement of Lisa O. Monaco
Assistant Attorney General
National Security Division
U.S. Department of Justice

Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

“Countering Terrorist Financing: Progress and Priorities”
September 21, 2011

Chairman Whitehouse, Ranking Member Kyl, and members of the Subcommittee, thank you for inviting me to testify today regarding the Department of Justice’s role in combating terrorist financing. The Department of Justice’s efforts to combat terrorism are closely coordinated with those of our interagency partners, some of whom are testifying with me here today. Our common objective is to deploy the counter terrorist financing tools available to the United States in a coordinated, integrated fashion to effectively disrupt the flow of funds and other material support to terrorist organizations.

The Department of Justice’s efforts in this regard fall generally into three categories, each of which I’ll address briefly today: our capacity building and technical assistance efforts with foreign governments; our participation in and defense of terrorist financing laws, regulations, and processes; and our investigation and prosecution of the individuals and networks involved in financing and supporting terrorism.

Capacity Building and Technical Assistance

Like our interagency colleagues, we at DOJ recognize that to be truly effective our counter terrorist finance efforts must be reinforced by other countries around the world. We have worked hard to help foreign governments develop their laws and capability to implement these laws for investigating and prosecuting terrorist financing to ensure that no jurisdiction provides a safe haven for the financial networks that support terrorist organizations. DOJ currently has State Department funded Resident Legal Advisers in Bangladesh, Kenya, Turkey, and the United Arab Emirates who are focused primarily on terrorist financing. In addition, DOJ’s network of 55 RLAs in countries around the world regularly provide technical assistance to the host government on terrorist financing laws and prosecutions.

In addition, DOJ has provided bilateral technical assistance to a number of foreign countries drafting or updating their counter terrorist finance laws, including Indonesia, Turkey, and Nigeria. We have also supported or assisted in scores of terrorist financing trainings around the world, including in Indonesia, Saudi Arabia, Yemen, Jordan, Azerbaijan, Turkey, and many other countries. The networks that finance and support terrorist organizations are international,
and our efforts effectively to disrupt those networks and bring their members to justice therefore rely critically on cooperation with capable foreign partners.

**Review and Defense of Terrorist Finance Designations**

The Department of Justice also participates in the designation of Foreign Terrorist Organizations (FTO); Specially Designated Terrorists (SDT); and Specially Designated Global Terrorists (SDGT) and defends in litigation the laws and regulations that permit designation and outlaw the provision of financing and other forms of material support to terrorist organizations.

The terrorism-related designations process in the United States plays a critical role in our fight against terrorist financing and is an effective means of curtailing support for terrorist activities based on listing entities and individuals the government has identified as terrorists, terrorist organizations, or supporters of terrorism or terrorist organizations. There are three principal mechanisms through which the executive branch designates individuals, entities, or organizations as involved in terrorism: under the Antiterrorism and Effective Death Penalty Act (AEDPA) of 1996; under Executive Order 12947, Prohibiting Transactions With Terrorists Who Threaten To Disrupt the Middle East Peace Process (Executive Order 12947), and under Executive Order 13224, Blocking Property And Prohibiting Transactions With Persons Who Commit, Threaten To Commit, Or Support Terrorism (Executive Order 13224). Executive Orders 12947 and 13224 were issued pursuant to the International Economic Emergency Powers Act (IEEPA).

AEDPA and Executive Orders 12947 and 13224 each prescribe procedures whereby executive officials may make terrorism-related designations. AEDPA gives the Secretary of State the authority to designate FTOs. Executive Orders 12947 and 13224 give the Secretaries of State and of the Treasury the authority to designate SDTs and SDGTs, respectively. Under both, the lead agency (either the State Department or the Department of the Treasury) compiles a record of classified and unclassified information supporting the designation. Moreover, both AEDPA and the Executive Orders require the lead agencies to consult with DOJ on the basis of this record in making the designation.

Specifically, Department of Justice attorneys closely review the administrative record compiled for purposes of designating an entity as an FTO, an individual or entity as an SDT or SDGT, to ensure that the record adequately supports the factual findings required by the applicable authority and to assess litigation risk in the event that a designation is subsequently challenged by the designated individual or entity.

Designation under the AEDPA or the Executive Orders introduces the possibility of a range of criminal and civil penalties as well as actions blocking and, potentially, confiscating the assets of the designee. Once an organization has been designated as an FTO under the AEDPA, knowingly providing material support or resources to that organization triggers criminal liability. It is also a criminal offense knowingly to receive military-type training from or on behalf of any organization designated as an FTO at the time the training takes place. FTO designation also has immigration consequences and financial repercussions, including blocking orders, forfeiture actions, and civil fines.
Designation pursuant to Executive Order 12947 or 13224 also blocks the property and interests in property of the SDTs or SDGTs, respectively, and prohibits U.S. persons from engaging in transactions with the designated individual or entity. Similarly, once an individual or entity has been designated an SDT or SDGT it is criminal to engage willfully in any transaction with such an individual or entity.

The Justice Department has defended a number of the components of this counterterrorist finance legal framework against constitutional and other challenges in litigation. Last year, in the Supreme Court case of Holder v. Humanitarian Law Project, the Department of Justice successfully defended provisions of the material support statute against claims that it was unconstitutional. Although the statutory provisions constituting “material support” challenged in that litigation included the provision of “personnel,” “training,” “service,” and “expert advice and assistance,” as I know the Subcommittee is aware, this material support law also prohibits the provision of any property, currency, monetary instruments, or financial securities. The Court, in an opinion authored by Chief Justice Roberts and joined by five other Justices, held that the material support statute was not unconstitutionally vague for purposes of the Due Process Clause and did not violate plaintiff’s constitutional rights of free expression and association.

The Department has also prevailed against challenges in litigation to the provision of AEDPA that grants the Secretary of State authority to designate organizations as FTOs.

We have also defended against constitutional challenges designations as SDGTs and other actions taken by the Department of the Treasury under IEEPA and Executive Orders 12947 and 13224. Persons and entities designated under those Executive orders can challenge their designations under the Administrative Procedure Act in district courts. We have successfully defended cases involving the Global Relief Foundation, the Holy Land Foundation, and the Islamic American Relief Association. (We are currently litigating cases involving the Al Haramain Foundation and Kindhearts.)

In sum, the Justice Department, in close coordination with our interagency partners, both participates in the designation processes and defends against challenges in litigation to the counterterrorist finance legal framework that supports the government’s authority to make such designations.

Investigation and Prosecution of Terrorist Financiers

At its heart, the government’s counter terrorist finance efforts take aim at the monetary and material support terrorist groups need to sustain themselves and to plot and carry out attacks against innocent civilians. We must disrupt the networks that provide such support, often referred to as the lifeblood of international terrorist organizations, whether the support they provide comes in the form of currency, training, valuable equipment, or any of the other categories of material support proscribed by our criminal laws. As the Supreme Court noted in Holder v. Humanitarian Law Project, there is “persuasive evidence” that providing “material support to a designated foreign terrorist organization – even seemingly benign support – bolsters the terrorist activities of that organization.”
Acting Assistant Director Ralph Boelte mentioned in his testimony the 2011 guilty plea of Mohammad Younis, whose unlicensed money transmitting business was used to transfer money to Faisal Shahzad to fund his attempt to detonate a car bomb in Times Square, and of Abdul Tawala Ibn Ali Alishtari, who pled guilty to terrorist financing charges and was sentenced to 10 years for facilitating the transfer of more than $150,000 to support terrorist training camps in Afghanistan and Pakistan. Let me mention a couple of other significant terrorist financing prosecutions.

- In October 2004, Abdurahman Alamoudi pled guilty and was sentenced to 23 years in prison for conduct that included facilitating the transfer of hundreds of thousands of dollars to a group plotting the assassination of Saudi Crown Prince Abdullah.
- In May 2009, five leaders of the Holy Land Foundation for Relief and Development were sentenced to terms ranging from 15 to 65 years for providing financial and other material support to Hamas. These cases are currently on appeal.
- There are currently a number of cases charged and pending in the United States regarding the alleged transfer of funds to Al Shabaab terrorists in Somalia.

We have also brought a number of cases under Section 960A of Title 21, the narcotics-terrorist statute, to disrupt individuals and networks attempting to use narcotics proceeds to finance terrorist organizations such as the Revolutionary Armed Forces of Colombia (or FARC), the Taliban, and al Qaeda in the Islamic Maghreb. And we have prosecuted individuals for trying to conceal the financial interest that SDGTs maintained in their companies, Infocom and PTech, thus cutting off a potential source of funding and money laundering for such SDGTs.

As the result of a close working relationship between our prosecutors and our partners in the law enforcement and intelligence communities, we have been able to disrupt these and other attempts to finance terrorism, gain valuable information as a result of the cooperation of the defendants, and bring the defendants to justice, ensuring that they are safely behind bars in American prisons, not continuing to finance terrorist attacks against America and our foreign partners.

Conclusion

As you have heard from all of my colleagues, United States Government efforts to counter terrorist financing have had some significant success over the past decade, but we have work yet to do. Terrorist organizations and their supporters continue to adapt and evolve their operations. To continue to be effective, we must continue to work with you to ensure that we have the authorities and capabilities necessary to effectively to counter terrorist financing. Thank you.
The Criminal Justice System as a Counterterrorism Tool: A Fact Sheet

The Obama administration is committed to using every instrument of national power to fight terrorism—including intelligence and military operations as well as the criminal justice system. As a counterterrorism tool, the criminal justice system has proven incredibly effective in both incapacitating terrorists and gathering valuable intelligence from and about terrorists. In every instance, the administration will use the tool that is most effective for fighting terrorism, and will make those decisions based on pragmatism, not ideology.

I. Intelligence Collection

The criminal justice system has been the source of extremely valuable intelligence on al-Qaeda and other terrorist organizations. The criminal justice system provides powerful incentives for suspects to provide accurate, reliable information, and the Department of Justice and FBI work closely with the rest of the intelligence community to maximize information and intelligence obtained from each cooperative. Below are just a few public examples.

Cooperators Provide Intelligence on al-Qaeda and Other Terror Groups

- L'Houssaine Kherchtou, who was arrested, Mirandized, charged with terrorism offenses, and cooperated with the government, provided critical intelligence on al-Qaeda. He testified in 2001 against four al-Qaeda members who were later sentenced to life in prison after being convicted in connection with the East Africa Embassy bombings.
- After his capture in Afghanistan, John Walker Lindh pleaded guilty in 2002 to supporting the Taliban and, as part of his plea agreement, provided valuable intelligence about training camps and fighting in Afghanistan.
- Mohammed Junaid Babar, arrested in 2004 for supporting al Qaeda and plotting attacks in the United Kingdom, has provided intelligence on terrorist groups operating along the Afghanistan/Pakistan border and has testified in the successful trials of terrorists in the United Kingdom and Canada. He is scheduled to testify in another terrorism trial in New York later this year.
- David Headley, arrested in 2009 and charged in connection with a plot to bomb a Danish newspaper and his alleged role in the November 2008 terror attacks in Mumbai, has provided extremely valuable intelligence regarding those attacks, the terrorist organization Lashkar y Ta’uiba, and Pakistan-based terrorist leaders.
- Adis Medunjanin, an alleged associate of Najiburrah Zazi, was taken into custody in January 2010, and, after waiving his Miranda rights, provided detailed information to the FBI about terrorist-related activities of himself and others in the United States and Pakistan. He has been charged with conspiring to kill U.S. nationals overseas and receiving military-type training from al-Qaeda.
- Other law enforcement cooperators are currently providing important intelligence regarding terrorist activity from East Africa to South Asia and regarding plots to attack the United States and Europe.

II. Incapacitating Terrorists

Hundreds of terrorism suspects have been successfully prosecuted in federal court since 9/11. Today, there are more than 300 international or domestic terrorists incarcerated in U.S. federal prison facilities. Events over the past year demonstrate the continuing value of federal courts in combating terrorism. In 2009, there were more defendants charged with terrorism violations in federal court than in any year since 9/11.

Past Terrorism Convictions and Recent Terrorism Indictments

- Richard Reid was arrested in December 2001 and convicted pursuant to a guilty plea in October 2002 of attempting to ignite a shoe bomb while on a flight from Paris to Miami carrying 184 passengers and 14 crewmembers. He is serving a life prison term.
- Ahmed Omar Abu Ali was convicted in November 2005 of conspiracy to assassinate the U.S. President and conspiracy to commit air piracy and conspiracy to destroy aircraft. Ali was sentenced to 30 years in prison.
• In May 2006, Zacarias Moussaoui was sentenced to life in prison after pleading guilty to various terrorism violations, admitting that he conspired with al-Qaeda to hijack and crash planes into prominent U.S. buildings as part of the 9/11 attacks.

• In September 2009, Najibullah Zazi was charged with conspiring to use a weapon of mass destruction as part of an al-Qaeda plot bomb targets in the United States. Several of his alleged associates have been arrested and charged in federal court.

• During 2009, 14 individuals were charged in the District of Minnesota connection with an ongoing investigation of individuals who have traveled from Minnesota to Somalia to train with or fight on behalf of the terrorist group al-Shabaab.

• In September 2009, Daniel Patrick Boyd and others were charged with plotting an attack on U.S. military personnel at the Quantico Marine Base, as well as recruiting young people to travel overseas in order to kill.
Thank you, Robert [Raben], for those kind words — and for the guidance, support, and friendship that you have provided to me for so many years. In fact, when I think of how long we’ve known each other, I’m especially grateful for the stories that you left out.

I also want to thank ACS’s visionary founder, Peter Rubin; its enthusiastic Executive Director, Caroline Fredrickson; its strong circle of supporters, including my friends at Covington and Burling; and its impressive, constantly expanding network of members. Over the last decade, this organization has become a powerful, critical voice in our nation’s most consequential discussions and debates. You have worked to ensure that the principles we hold most dear always trump calls for expediency or contests for political popularity. You have helped to safeguard our democracy and to strengthen our legal system. You’ve raised awareness about an impending crisis — and an alarming rate of vacancies — in our federal judiciary. You have challenged policymakers to address this — and made the case that highly qualified, capable individuals nominated by the President should have the chance to serve their country, in government posts and on the federal bench. And you have created a meeting ground for some of our nation’s most talented and insightful leaders and lawyers — and for thousands of young attorneys and students who give us all great hope for the future that we will share and — together — that we must build.

It is a pleasure to be with you all. And it’s an honor to be invited, once again, to participate in this annual convention.

In June of 2008 — the summer before I became Attorney General and Barack Obama became our President — I stood before you. And I joined with many of you in lamenting the fact that, with respect to its commitment to the Constitution and to the rule of law, our government had lost its way.

That evening, even as our shared concerns weighed heavily upon us, there was a palpable sense of hope; a common faith that — despite the odds against us and the challenges before us — our nation could correct course, just as it always has — even during some of the darkest moments in our constitutional history.

Three years later — although the struggle has been far more difficult than anyone might have predicted, and although some of you have not agreed with every decision this Administration has made — I am pleased to report that, as a nation, we have begun to find our footing once again. This Administration is moving in a direction that is guided, not by fear — but by fact, by reason, and by a commitment to advancing the cause of justice and to upholding our nation’s most essential and enduring values.

In this work, I am extremely proud of the contributions that the Department of Justice has made.

Over the last two years, we’ve taken meaningful steps to prevent and combat terrorism, violent crime, and financial fraud. And we’ve identified innovative, collaborative ways to protect the
most vulnerable members of our society, as well as the law enforcement officers who keep us all safe.

In addition to these priority areas, we’ve advanced our fight against international crime networks, drug cartels, gangs, and cyber criminals — and pushed those who have the power to reduce today’s unacceptable backlog of judicial nominations to take action — and to do the right thing. We’ve also focused on safeguarding our environment — and acted quickly to respond to, and to seek justice for those affected by, the largest oil spill in U.S history. And we’ve successfully advocated for greater fairness in our sentencing policies — work that continues in our current efforts to ensure that reductions in the unjust disparity between crack and powder cocaine offenses are applied retroactively.

But, tonight, I’m especially pleased to report that we have reinvigorated the important work of our Civil Rights Division. Not only is this office once again open for business — it has never been stronger.

As some of you know, during this Administration’s first fiscal year, the Department filed a record number of civil rights criminal cases. The following year, we broke this record. In recent months, we’ve prosecuted the largest human trafficking case in history — and, just yesterday, secured guilty pleas from three defendants. We have addressed more than 100 open matters under the landmark Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act — critical legislation that so many of us, including Senator Whitehouse and Congressman Conyers, worked tirelessly to move forward. The Department has secured the first convictions under this new law. We’ve also expanded enforcement efforts to guarantee that — in our workplaces and military bases; in our housing and lending markets; in our voting booths and border areas; in our schools and places of worship — the rights of all Americans are protected.

In addition to strengthening this essential division, the Department has established an entirely new component — our Access to Justice Office. This groundbreaking initiative was launched last year — with the help and leadership of one of ACS’s most dedicated members, our dear friend, Larry Tribe. The work that’s currently underway in this office — which now is being led by Senior Counselor Mark Childress, who I’m glad is here with us tonight — reflects an historic assurance that, at long last, expanding access to legal services is — and will continue to be — a national priority.

Many of you have shown extraordinary support for the goals of this initiative. And I have no doubt that, with your continued partnership, we can build upon the progress it has made in protecting funding for — and expanding access to — legal services, and raising awareness about the challenges that current — and future — lawyers must help to address. While I’m not naive about today’s budget limitations, I am confident that we can find the solutions that we need to ensure the integrity of our legal system and to honor the promise of equal justice for all.

Beyond this work, I am proud — and every citizen, every steward of our justice system, and every member of our nation’s legal community can be encouraged — that, in fulfilling our paramount responsibility to protect the American people, the Justice Department has led with strength and by example. Even as we’ve confronted unprecedented, and increasingly sophisticated, national
security threats, we’ve made historic progress – without giving in to fear, or compromising our values as Americans.

Of course, we have not won every argument. We have not achieved some of our goals as quickly as we would have liked. And, although we have pledged to use every tool available to keep the American people safe, attempts have been made to tie our hands and limit our options.

The American people deserve better. That’s why we must demand more – from our policymakers, from our fellow citizens, and from ourselves.

It will take a collective effort – and collaboration between partners inside and outside of government – to reestablish our nation’s moral authority, to reaffirm our guiding principles, to rid our public dialogue about these issues of fear mongering, and to remove politics from prosecutorial determinations.

Politics has no place – no place – in the impartial and effective administration of justice. Decisions about how, where, and when to prosecute must be made by prosecutors, not politicians. And this is true for every case, whether it involves brutal terrorists or white collar criminals.

So long as I am privileged to serve as Attorney General, I will defend the exclusive right of the Executive Branch to determine appropriate venues and mechanisms for all criminal trials. And I will continue to point out one indisputable fact, which has been proven repeatedly, during this Administration and the previous one: in disrupting potential attacks and effectively interrogating, prosecuting, and incarcerating terrorists – there is, quite simply, no more powerful tool than our civilian court system.

Despite this fact, some in Congress have proposed to ban the use of Article III courts in prosecuting terrorism-related cases. They claim that utilizing our civilian court system – as we have for more than 200 years – would somehow jeopardize public safety.

I don’t need to be told – by anyone – about the seriousness of the dangers we face. I begin each day with a briefing on the most urgent threats made against the United States in the preceding 24 hours. I know that – in distant countries, and within our own borders – there are people intent on, and actively plotting to, kill Americans.

For nearly as long as your organization has existed, our nation has been at war. And like every person in this room, like the President and those who serve this Administration, and like every Member of Congress, I am determined to defeat our enemies. I know we can, and I am certain we will. But victory and security will not come easily. And they won’t come at all if we adhere to a rigid ideology, adopt a narrow methodology, or abandon our most effective terror-fighting weapon – our Article III court system.

Despite this reality, we continue to see overheated rhetoric that is detached from history – and from the facts. We see crucial national security tools, once again, being put at risk by those who disparage the American criminal justice system, and misguided claim that terror suspects cannot be tried safely in our civilian courts.
Here are the facts: Every single suspected terrorist captured on American soil — before and after the September 11th attacks — has first been taken into custody by law enforcement — not the United States military. Our criminal justice system has proven — time and again — that it provides all the authority and flexibility we need to effectively combat terrorist threats. Since 9/11, hundreds of individuals have been convicted of terrorism or terrorism-related offenses in civilian courts.

Not one of these individuals has escaped custody. Not one of the judicial districts involved has suffered retaliatory attacks. And not one of these terrorists arrested on American soil has been tried by a military commission. Not by the Obama Administration — and not by the Bush Administration. Not a single one.

Even though excellent work has been done to improve and reform the military commissions, these tribunals are largely untested. Without civilian law enforcement and Article III courts, our ability to disrupt, dismantle, and defeat terror plots; to secure actionable intelligence; to enlist international cooperation; and to punish those who have — and who intend to — harm Americans would be seriously damaged.

For these reasons, we must speak out. And we must set the record straight. In this work, I pledge my own best efforts. And, tonight, I ask for yours.

We cannot — and we must not — allow the public safety concerns that all Americans share to divide us — or to compromise the principles that have always defined and distinguished our nation, and our people.

Together, we must stand up for the values enshrined in our Constitution. And we must ensure that the rule of law — which, for more than two centuries, has held this nation together and made America an example for all the world — is not seen as an obstacle to be overcome. Instead, it must be recognized as the foundation for our continued security — and our future progress.

Achieving this goal is our collective responsibility. And it must become our common cause. So, tonight, as we reflect on the ideals that have defined our history and will determine our destiny, let us also recommit ourselves to honoring our most sacred principles — in the work that we do each day, and in our ongoing pursuit of a more secure, more just, and more perfect union.

Thank you.
Law Enforcement as a Counterterrorism Tool

David S. Kris*

In January 2011, Congress enacted legislation prohibiting the use of federal funds to transfer to the United States any individuals currently detained at Guantánamo Bay, Cuba. Among the purposes of this provision, observers commented, was to prevent the prosecution of these detainees in federal court in the United States. President Obama signed the legislation into law as part of the Defense Authorization Act, but he also issued a statement strongly objecting to the provision and pledging to seek its repeal:

[This provision] represents a dangerous and unprecedented challenge to critical executive branch authority to determine when and where to prosecute Guantánamo detainees, based on the facts and the circumstances of each case and our national security interests. The prosecution of terrorists in Federal court is a powerful tool in our efforts to protect the Nation and must be among the options available to us. Any attempt to deprive the executive branch of that tool undermines our Nation's

* Assistant Attorney General for National Security at the U.S. Department of Justice from March 2009 to March 2011. This article was written and submitted for publication when Mr. Kris was Assistant Attorney General. The views expressed herein do not necessarily reflect the views of the U.S. Government. Brad Wiegmann and Rosemary Nidiry provided superb assistance on this project. Some of the points made in this article expand on remarks made by Mr. Kris in a speech at the Brookings Institution in June 2010. The prepared remarks are available on both the Department of Justice's website, http://www.justice.gov/ndp/ops/pr/speches/2010/nsd-speech-100611.html, and on Brookings' website, http://www.brookings.edu/events/2010/0611_law_enforcement.aspx. Video of the speech is available on C-SPAN's website, http://www.c-spanvideo.org/program/294017-1.

1. See The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, H.R. 6523, 111th Cong. §1052, enacted as Pub. L. No. 111-383 (Jan. 7, 2011). During the spring of 2011, other bills with similar provisions were pending in Congress. For example, Sections 1039 and 1046 of H.R. 1540, the National Defense Authorization Act for Fiscal Year 2012, which was passed by the House of Representatatives on May 26, 2011, would prohibit Defense Department appropriated funds for 2012 from being used to “transfer or release an individual detained at Guantánamo . . . to or within the United States,” and require trial by military commission for certain terrorists if they are “subject to trial . . . by a military commission.”

2. See, e.g., David B. Rivkin, Jr., & Lee A. Casey, Editorial, The Wrong Way To Stop Civilian Terror Trials, WALL ST. J., Dec. 21, 2010, at A17 (noting that the apparent purpose of the defense authorization provision is to prevent the prosecution of Guantánamo Bay detainees in federal court).

counterterrorism efforts and has the potential to harm our national security. 4

The Congressional action and the President’s response are part of a broader public debate about the role of law enforcement as a counterterrorism tool. Some question the effectiveness of the U.S. criminal justice system and argue that it should never be used against terrorists, or at least some kinds of terrorists. In contrast, some others argue that law enforcement is the only legitimate way to detain terrorists, and that they should either be prosecuted in the civilian courts or released. 5

This article argues that we should continue to use all of the military, law enforcement, intelligence, diplomatic, and economic tools at our disposal, selecting in each case the particular tool that is most effective under the circumstances, consistent with our laws and values. The discussion proceeds in five main parts.

Part I reviews the recent history of our national counterterrorism strategy, focusing in particular on the origins and evolution of the Justice Department’s National Security Division (NSD), which I led from March 2009 until March 2011. 6 Knowing a little about NSD is important because NSD is a key part of how the country came to a consensus, at least until recently, about the appropriate role of law enforcement as a counterterrorism tool.

Part II sketches a conceptual framework for thinking about the role of law enforcement in the current conflict, and more generally as a counterterrorism tool. The idea here is to identify the right questions, and the right way of approaching the policy debate in which we are now engaged as a country. Identifying the right questions is difficult but important.

Part III answers the questions posed in Part II. It briefly describes some of the empirical evidence about how law enforcement has been used to

---

4. Id.
5. See, e.g., Benjamin Weiser, Top Terror Prosecutor Is a Critic of Civilian Trials, N.Y. TIMES, Feb. 19, 2011, available at http://www.nytimes.com/2010/02/20/national/20prosecutor.html (quoting Andrew McCarthy, formerly an Assistant U.S. Attorney, as saying, “A war is a war. A war is not a crime, and you don’t bring your enemies to a courthouse.”). However, McCarthy has supported enhancements to the criminal justice system designed to make it more effective against some terrorists in the post-9/11 era. See, e.g., Material Support to Counterterrorism, NATIONAL REVIEW ONLINE, Dec. 14, 2004, available at http://www.nationalreview.com/articles/213131/material-support-counter-terrorism/andrew-c-mccarthy). On the other side of the debate, the ACLU has argued: “If the government has enough credible evidence against a detainee, it should prosecute him in a federal court, which are [sic] well positioned to accommodate the government’s legitimate national security interests without compromising the fundamental rights of defendants. Where there is not, detainees should be repatriated to their home countries or, if there is a risk of torture or abuse, transferred to countries where human rights will be respected.” See www.closegimno.com.
combat terrorism, and, in particular, how it has been used to disrupt plots, incapacitate terrorists, and gather intelligence. This serves as the basic, affirmative case for retaining law enforcement as one of our counterterrorism tools. Part III also explores some of the arguments against using law enforcement for counterterrorism, and explains why (in my view) those arguments are wrong. Part III closes with a discussion of pragmatism and perception, and the role of values in counterterrorism.

Part IV offers a comparison between civilian law enforcement, detention under the law of war,\(^7\) and prosecution in a military commission. We need such a comparison to make smart decisions about public policy as well as decisions about the disposition of individual cases. The chief goal of Part IV is to explain the major pros and cons of each system.\(^8\)

Finally, Part V discusses how law enforcement can be made more flexible and more effective as a counterterrorism tool. In particular, it addresses how the public-safety exception to Miranda should apply in the context of terrorism investigations.\(^9\)

\section{THE RECENT HISTORY OF LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL}

We often hear that before 9/11, the United States took a "law enforcement approach" to counterterrorism.\(^10\) There is some truth in that, but I think it oversimplifies the situation. In fact, the 9/11 Commission

\(^7\) Law of war detention as used in this paper refers to detention pursuant to the Authorization for Use of Military Force (AUMF), Pub. L. No. 107-40, 115 Stat. 224 (2001), as informed by law of war principles. The procedural discussion on law of war detention focuses on any such detention that has been held to be subject to habeas corpus.

\(^8\) There are two appendices to this article: Appendix 1 is a description of some of the significant cooperation and intelligence activities of terrorist groups that the U.S. government has obtained from terrorism suspects via the criminal justice system. Appendix 2 is a chart comparing the criminal justice system and the reformed system of military commissions and law of war detention.

\(^9\) Miranda v. Arizona, 384 U.S. 436, 479 (1966); see New York v. Quarles, 467 U.S. 649, 655-56 (1984) (finding a public safety exception to the requirement of Miranda warnings where law enforcement is acting to protect the public and that the availability of that exception does not depend on the motivation of the individual officers involved).

\(^10\) See, e.g., Oversight of the U.S. Department of Justice: Hearing Before the S. Comm. on the Judiciary 111th Cong. (June 17, 2009) (statement of Sen. Jeff Sessions), available at http://judiciary.senate.gov/hearings/testimony.cfm?id=3913&stid=515 (expressing concern that Department of Justice "would operate under [a] pre-9/11, criminal law mindset when fighting terrorists"); Andrew C. McCarthy, Kerry's Exaggerated Terror Problem, NAR'L REV. ONLINE (Mar. 30, 2004), http://fold.nationalreview.com/comment/mccarthy200403300888.asp ("In the eight years from 1993 to 2001, when terrorism was regarded as a law enforcement issue, we managed to prosecute about 40 terrorists in trials that generally took six months or more, and terrorist attacks nevertheless continued apace. On the other hand, since October 2001, our military has killed or captured thousands of terrorists and there have been no domestic attacks."); Peter D. Feaver, The Clinton Mind-Set, WASH. POST, Mar. 24, 2004, at A21.
found that before 9/11, "the CIA was plainly the lead agency confronting al Qaeda"; law enforcement played a "secondary" role; and military and diplomatic efforts were "episodic." I was involved in national security before 9/11, and that seems roughly accurate to me.

After 9/11, of course, all of our national security agencies ramped up their counterterrorism activities. As our troops deployed to foreign battlefields and the Intelligence Community expanded its operations, the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) also evolved. We began with the important legal change of tearing down the so-called "FISA wall," under which law enforcement and intelligence were largely separate enterprises and law enforcement was correspondingly limited as a counterterrorism tool.\(^1\)

The Foreign Intelligence Surveillance Act, or FISA, is a federal statute enacted by Congress in 1978 that governs electronic surveillance and physical searches of foreign intelligence targets in the United States.\(^2\) It is an extremely powerful investigative tool, and one that is vitally important to our national security. FISA does not allow, and never has allowed, surveillance or searches of ordinary criminals like Bonnie and Clyde. It applies only to foreign intelligence threats, such as Robert Hanssen or Osama bin Laden. Under the FISA wall, however, intelligence and law enforcement had to remain relatively separate even with respect to investigations of spies and international terrorists. In other words, the price of using FISA — or preserving the option to use FISA — was a requirement to keep law enforcement and intelligence at arm’s length.\(^3\) In some cases, for example, parallel law enforcement and intelligence investigations of the same terrorism targets had to be run by separate squads of FBI agents.

This wall was built on the premise that a powerful intelligence tool like FISA should not be used for the primary purpose of supporting criminal prosecution, even if that prosecution targeted terrorists (as opposed to ordinary criminals). It was derived in part from an interpretation of the FISA statute and the Fourth Amendment.\(^4\) Proponents of the wall recognized that FISA could be used to gather information needed to neutralize terrorists through intelligence, diplomatic, or military action; but

---

11. NATIONAL COMMISSION ON THE TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 400-401 (2004), available at http://www.gpoaccess.gov/911/pdf/fullreport.pdf ("Before 9/11, the CIA was plainly the lead agency confronting al Qaeda. The FBI played a very secondary role. The engagement of the departments of Defense and State was more episodic. Today the CIA is still central. But the FBI is much more active, along with other parts of the Justice Department. The Defense Department effort is now enormous.").


14. See Rise and Fall, supra note 12.

15. Id.
they treated law enforcement efforts to neutralize terrorists as a separate undertaking. Thus, for example, while FISA could (at least in theory) be used for the primary purpose of collecting information to allow the Department of Defense (DoD) to locate, target, and capture or kill a terrorist on the battlefield abroad, it could not be used for the primary purpose of collecting information to allow the DOJ to prosecute, convict, incarcerate, or execute a terrorist in the United States. The wall limited information-sharing and coordination between intelligence officers and law enforcement officers, and this hindered efforts to combat terrorism.

The demise of the FISA wall reflected, and also reinforced, the conclusion that law enforcement helps protect national security. This is not to say that law enforcement is the only way to protect national security, or even that it is the best way. But I do believe we came to a national consensus, in the years immediately after 9/11, that law enforcement is one important way of protecting national security. Some of the evidence for that conclusion is set out below.

The wall came down as a result of combined legislative, executive, and judicial decisions — including the USA PATRIOT Act, new Attorney General Guidelines, and an unprecedented decision of the Foreign Intelligence Surveillance Court of Review. When Congress enacted the PATRIOT Act, it included a provision making clear its view that law enforcement protects against terrorism. Section 504 of the Act provided explicitly that intelligence officials using FISA "may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against . . . international terrorism," reflecting an understanding that both intelligence and law enforcement officials in fact play a protective role in counterterrorism efforts. As Senator Patrick Leahy explained at the time, "consultation and coordination is authorized for the enforcement of laws that protect against international terrorism," and, indeed, "the use of FISA to gather evidence for the enforcement of these laws was contemplated" in 1978 when the statute was first enacted.

16. See 9/11 COMMISSION REPORT, supra note 11, at 78-79 (describing legal constraints on the FBI and origins of "the wall"); Rise and Fall, supra note 12.
17. See 9/11 COMMISSION REPORT, supra note 11, at 270-72 (describing how "the wall" hampered efforts to investigate and locate some of the 9/11 hijackers).
In its effort to tear down the wall in 2002, the government relied on the PATRIOT Act to argue to the Foreign Intelligence Surveillance Court of Review that “[p]rosecution is often a most effective means of protecting national security.” It explained that while FISA was designed to acquire information necessary to “protect” against international terrorism and other threats to national security, the statute did “not limit how the government may use the information to achieve that protection. In other words,” the government argued, “the [law] does not discriminate between protection through diplomatic, economic, military, or law enforcement efforts.” The government’s claims on this topic included an example of how law enforcement helps protect against terrorism:

[T]he recent prosecution of Ahmed Ressam, who was charged with attempting to destroy Los Angeles International Airport, protected the United States by incapacitating Ressam himself from committing further acts, and by deterring others who might have contemplated similar action. Moreover, as a result of his conviction and sentence, Ressam agreed to cooperate with the government and provided information about the training he received at an al Qaeda camp overseas. That kind of prosecution thus protects the United States directly, by neutralizing a threat, and indirectly, by generating additional foreign intelligence information.

The court agreed strongly with the idea that law enforcement can both neutralize terrorists and obtain intelligence from them:

The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power [such as an international terrorist group] may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity. The government might wish to surveil the agent for some period of time to discover other participants in a conspiracy or to uncover a foreign power’s plans, but typically at some point the government would wish to apprehend the agent and it might be that only a prosecution would provide sufficient


22. Id. (emphasis in original).

23. Id. at 35.
incentives for the agent to cooperate with the government. Indeed, the threat of prosecution might be sufficient to "turn the agent."\(^{24}\)

In 2005, the bi-partisan Weapons of Mass Destruction (WMD) Commission -- co-chaired by one of the judges from the Foreign Intelligence Surveillance Court of Review\(^{25}\) -- reported to the President that "the Department of Justice's primary national security elements . . . should be placed under a new Assistant Attorney General for National Security."\(^{26}\) The Report went on to explain that "this Assistant Attorney General would serve as a single focal point on all national security matters. The Assistant Attorney General would be responsible for reviewing FISA decisions and determining what more can be done to synthesize intelligence and law enforcement investigations."\(^{27}\) The core idea was that this "synthesis" of intelligence and law enforcement would make the government more effective against terrorists.

Shortly thereafter, President Bush endorsed the WMD Commission's recommendation, explaining that "the United States Department of Justice has a vital role in the protection of the American people from threats to their security, including threats of terrorist attack."\(^{28}\) Congress responded in 2006 by creating the National Security Division,\(^{29}\) noting that doing so was

\(^{24}\) In re Sealed Case, 310 F.3d at 724.

\(^{25}\) Judge Laurence Silberman of the U.S. Court of Appeals for the D.C. Circuit.


\(^{27}\) Id. at 473.

\(^{28}\) See Memorandum from the President for the Vice President, Sec'y of State, Sec’y of Def., Atty Gen., Sec’y of Homeland Sec., Dir. of Office of Mgmt. and Budget, Dir. of Nat'l Intelligence, Assistant to the President for Nat'l Sec. Affairs, and Assistant to the President for Homeland Sec'y and Counterterrorism (June 29, 2005), available at http://georgewbush-whitehouse.archives.gov/news/releases/2005/06/20050629-1.html.

\(^{29}\) See PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177, §506, 120 Stat. 192 (2006), codified in various sections of Titles 18 and 50 of the U.S. Code. During this same period following 9/11, Congress enacted other legislation supporting and enhancing the use of law enforcement as a counterterrorism tool. For example, in 2001 the PATRIOT Act added new terrorism offenses, enhanced existing offenses, stiffened penalties, and expanded extraterritorial jurisdiction. These included expanding the definition of terrorism, extending the statute of limitations of certain terrorism offenses, increasing the maximum penalties for certain terrorism offenses, making it a crime to harbor or conceal terrorists, criminalizing certain attacks on mass transit systems, expanding the biological weapons statute, and others. See PATRIOT Act, §§801-811. Congress also made numerous changes to FISA and other laws designed to enhance the FBI's ability to track and intercept potential terrorist communications and conduct searches for counterterrorism purposes. See id. §§201-219. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the FBI to "develop and maintain a specialized and integrated national intelligence workforce," see IRTPA §200(1)(e)(1), Pub. L. No. 108-458, 118 Stat. 3638 (2004), and the FBI responded by creating an Intelligence Career Service which more than doubled the
consistent with [the] recommendation by the WMD Commission. As the Senate Intelligence Committee explained in a report on a related bill, "NSD is expected to actively participate in the Intelligence Community's mission to prevent and otherwise neutralize threats to the national security," even though it also "should be considered a law enforcement agency, albeit one that specializes in the prevention, detection, investigation, neutralization, and prosecution of crimes that threaten the national security."

In September 2006, NSD was officially established with the swearing in of the first Assistant Attorney General (AAG) for National Security. By statute, the AAG is the Justice Department's liaison to the Director of National Intelligence, who heads the U.S. Intelligence Community, and by regulation NSD is charged with authority and responsibility to oversee prosecutions of federal crimes involving national security, administer FISA, develop and implement intelligence policy, and conduct legal oversight of intelligence activities. In the current era, federal prosecutors and other law enforcement officials enjoy the authority and the ability to participate fully in intelligence investigations and to cooperate with the Intelligence Community. More specifically—and of particular personal interest to me in my recent role as its AAG—NSD combines in one organizational unit both terrorism and espionage prosecutors and intelligence lawyers and professionals. Even adjusting for my bias, they are, I believe, working extremely well together to produce the synthesis, and the synergy, that will make the country safer.

number of intelligence analysts at the FBI since 9/11. See Concerning Implementation of the Intelligence Reform and Terrorism Prevention Act of 2004: Hearing Before the S. Select Comm. on Intelligence, 110th Cong. at 4 (Jan. 25, 2007) (statement of John S. Pistole, Deputy Dir. of the FBI), available at http://intelligence.senate.gov/070125/pistole.pdf. The IRTPA also further amended the key statutes prohibiting material support to terrorism or foreign terrorist organizations to expand their scope and ensure they could be applied extraterritorially. See IRTPA § 6603(b) (2004), amending 18 U.S.C. §§ 2339A and B. Two years later, in the USA PATRIOT Improvement and Reauthorization Act, Congress once again enacted new terrorism offenses and made other changes to enhance our arsenal of criminal laws targeting terrorist activity. These changes included, among others, adding offenses to the definition of federal crimes of terrorism, strengthening offenses punishing attacks on transportation systems, strengthening asset forfeiture provisions for terrorism-related offenses, and creating new offenses for transporting terrorists or dangerous materials to be used for terrorist purposes. See USA PATRIOT Improvement and Reauthorization Act, §§110-112, 305 (2005).

2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

Similarly, FBI Director Robert Mueller and the Attorneys General he has served since 2001 have integrated intelligence and law enforcement functions with respect to counterterrorism, and dramatically increased the FBI's resources and focus on intelligence collection and analysis.\textsuperscript{35} The FBI has long been the Intelligence Community element with primary responsibility for collecting and coordinating intelligence about terrorist threats in the United States,\textsuperscript{36} and since 9/11 it has made this mission its highest priority.\textsuperscript{37} The FBI now has a National Security Branch, comprised of the Counterterrorism Division, the Counterintelligence Division, a Directorate of Intelligence, and a WMD Directorate, as well as field intelligence groups in each of its 56 field offices, all of which put into practice FBI priorities and the emphasis on integration of criminal and intelligence efforts.\textsuperscript{38} These developments reflect the mainstream, consensus view that law enforcement - along with military, intelligence, and diplomatic efforts - helps protect national security. Obviously, developing this consensus was not easy: it required multiple, sequential action from all three branches of the federal government, and it took several years. Along the way, the process addressed concerns - sincerely held and strongly expressed - that the FISA wall was necessary to protect civil liberties, and that intelligence and law enforcement should remain distinct.\textsuperscript{39} In the end, those concerns, although sincere, appeared misguided, and the process showed, in


37. See, e.g., Confronting the Terrorist Threat to the Homeland: Six Years After 9/11: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs, 110th Cong. (Sept. 10, 2007) (statement of Robert S. Mueller, III, Dir., Fed. Bureau of Investigation), available at http://www2.fbi.gov/congress/congress07/mueller071007.htm ("In response to those attacks - and to other acts and threats of terrorism - the FBI realigned its priorities - making counterterrorism, counterintelligence, and cyber security its top three priorities - and shifted resources to align with those priorities. Since 9/11, the FBI has set about transforming itself into a national security agency, expanding our mission, overhauling our intelligence programs and capabilities, and undergoing significant personnel growth.").

38. See Statement of John S. Pistole, Deputy Dir. of the FBI, supra note 29, at 1, 3.

particular, that the demise of the wall and the increased involvement of law enforcement in counterterrorism did not threaten civil liberties, but did significantly enhance our national security.\footnote{See, e.g., The USA PATRIOT Act in Practice: Sheding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary, 107 Cong. (Sept. 10, 2002) (statement of David S. Kris, Assoc. Deputy Att’y Gen.), available at http://www.access.gpo.gov/congress/senate/pdf/107thrpt/87866.pdf, \textit{Rise and Fall}, supra note 12.} The consensus, I believe, was that national security was better achieved through law enforcement and intelligence together than through either alone.

Today, however, the consensus that emerged in the aftermath of 9/11 shows some signs of unraveling. We seem to be witnessing a resurgence of arguments to keep law enforcement out of counterterrorism. This time, however, the arguments are not coming from civil libertarians, but from the other side of the spectrum — those who are concerned about the \textit{effectiveness} of criminal justice in protecting national security. The arguments rest on the theory that law enforcement cannot — or should not — incapacitate or collect intelligence from suspected terrorists, and that we should treat all terrorists as military targets to be dealt with exclusively by military or intelligence agencies other than the FBI. The Obama administration supports the use of military commissions,\footnote{In 2009, the General Counsel of the Department of Defense, Jeh Charles Johnson, and I were the government’s chief witnesses in support of amendments to the Military Commissions Act that later became law. We testified before both the House and Senate Armed Services and Judiciary Committees. \textit{See On Legal Issues Regarding Military Commissions and the Trial of Detainees for Violations of the Law of War, Panel I: Hearing Before the S. Comm. on the Armed Servs., 111th Cong. (2009) (LexisNexis Congressional); The Military Commissions Act of 2006 and Detainee Policy: Hearing Before the H. Comm. on the Armed Servs., 111th Cong. (2009) (LexisNexis Congressional); Prosecuting Terrorists: Civilian and Military Trials for Guantanamo and Beyond: Hearing Before the Subcomm. on Terrorism and Homeland Sec. of the S. Comm. on the Judiciary, 111th Cong. (2009) (LexisNexis Congressional); Proposals for Reform of the Military Commissions System: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (2009) (LexisNexis Congressional). Here is an excerpt from my testimony before the House Armed Services Committee, supra: [A]s the President stated in his speech at the National Archives \textit{[see infra note 42]}, we need to use all elements of our national power to defeat our adversaries. And that is including, but not limited to, prosecution in both Article III courts and in military commissions. \ldots Article III courts, which have unquestioned legitimacy, are also effective in protecting national security; and military commissions, as we propose to reform them, which have unquestioned effectiveness, are also fair and legitimate. Now, I suspect that there are many people in this room, or perhaps elsewhere, who might agree only with the first part of the sentence that I just stated, and there will be others who agree only with the second part; but we think both parts are right.} and recognizes the need, at least in some cases, for detention (rather than prosecution) under the law of war.\footnote{As the President recognized in his speech at the National Archives on May 21, 2009, while the Administration is “going to exhaust every avenue that we have to prosecute those at Guantanamo who pose a danger to our country,” once the comprehensive review of
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

history, there is no question of excluding these weapons from our counterterrorism arsenal. The only question is whether to exclude law enforcement. I will turn to that question now.

II. A FRAMEWORK FOR EVALUATING THE ROLE OF LAW ENFORCEMENT IN COUNTERTERRORISM

As I understand it, the argument for excluding law enforcement from counterterrorism is basically the following:

(1) We are at war.

(2) Our enemies in this war are not common criminals.

(3) Therefore we should fight them using military and intelligence methods, not law enforcement methods.

This is a simple and rhetorically powerful claim, and precisely for that reason it may be attractive to some.43

In my view, however, and with all due respect, the argument is not correct. And it will, if adopted as policy, make us less safe. Of course, I do not contend that law enforcement is always the right tool for combating terrorism. But it is not the case that it is never the right tool. The reality, I think, is that it is sometimes the right tool.

And whether it is the right tool in any given case depends on the specific facts of that case. Here is my version of the argument:

(1) We are at war. The President and Attorney General have said this many times.44

all detainees at Guantánamo is completed, “there may be a number of people who cannot be prosecuted for past crimes, in some cases because evidence may be tainted, but who nonetheless pose a threat to the security of the United States,” and this Administration is “not going to release individuals who endanger the American people.” President Barack Obama, Remarks by the President on National Security (May 21, 2009), available at http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09.

43. This argument is not merely rhetorical. As noted in the introduction, in the 2011 Defense Department authorization legislation, Congress enacted a prohibition on the use of federal funds to transfer individuals currently detained at Guantánamo Bay to the United States for any purpose. See H.R. 6523, §1032, supra note 1. While this provision does not expressly prohibit federal civilian trials, its purpose at least in part may be to prevent such trials of these detainees from taking place. See, e.g., Rivkin & Casey, supra note 2.

44. In his inaugural address, the President said, “[o]ur nation is at war against a far-reaching network of violence and hatred,” and warned “those who seek to advance their aims by inducing terror and slaughtering innocents” that “we will defeat you.” The President’s inaugural address is available at http://www.whitehouse.gov/blog/inaugural-address. Similarly, in his speech at the National Archives in May 2009, the President
(2) In war, the goal is to win—no other goal is acceptable.

(3) To win the war, we need to use all available tools that are consistent with the law and our values, selecting in any case the tool that is best under the circumstances.

In other words, within the space defined by our values, we must be relentlessly pragmatic and empirical. We cannot afford to limit our options artificially, or yield to preconceived notions of suitability or “correctness.” We have to look dispassionately at the facts, and then respond to those facts using whatever methods will best lead us to victory.

Put in more concrete terms, we should use the tool that is best suited for the problem we face. When the problem looks like a nail, we need to use a hammer. When it looks like a bolt, we need to use a wrench. Hitting a bolt with a hammer makes a loud noise, and it can be satisfying in some visceral way, but it is not effective and it is not smart. If we want to win, we cannot afford to abandon the correct tool to solve the problem.

If you take this idea seriously, it complicates strategic planning, because it requires a detailed understanding of our various counterterrorism tools. If you are a pragmatist, focused relentlessly on winning, you cannot make policy or operational decisions at 30,000 feet. You have to come explained that his “single most important responsibility... is to keep the American people safe,” that “al Qaeda is actively planning to attack us again,” and that “we must use all elements of our power to defeat it.” Remarks by the President on National Security, supra note 42. On February 1, 2010, the President said, “it’s important to understand that we are at war against a very specific group—al Qaeda and its extremist allies,” that al Qaeda “is our target and... our focus,” and that “we have to fight them on all fronts.” Interview of President Barack Obama by YouTube at the White House (Feb. 1, 2010), available at http://www.whitehouse.gov/whitehouse/presidential/obama-youtube.

The Attorney General has made the same points many times. In his confirmation hearing on January 16, 2009, he said, “I don’t think there’s any question but that we are at war. And I think, to be honest, I think our nation didn’t realize that we were at war when, in fact, we were. When I look back at the ’90s and the Tanzanian—the embassy bombings, the bombing of the [U.S.S.] Cole, I think we as a nation should have realized that, at that point, we were at war. We should not have waited until September the 11th of 2001, to make that determination.” Nomination of Eric Holder To Be Attorney General in the Obama Administration: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (Jan. 16, 2009), available at http://judiciary.senate.gov/resources/hearings/111-transcripts.cfm. In a press conference held on February 22, 2010, he said that “we must use every weapon available to win [the war.]” Attorney General Eric Holder, Press Conference Announcing Guilty Plea by Najibullah Zazi (Feb. 22, 2010), available at http://www.justice.gov/ag/speeches/2010/ag-speech-100222.html. And in Congressional testimony given in November 2009, he said, “I know that we are at war. I know that we are at war with a vicious enemy who targets our soldiers on the battlefield in Afghanistan and our civilians on the streets here at home. I have personally witnessed that somber fact in the faces of the families who have lost loved ones abroad, and I have seen it in the daily intelligence stream I review each day.” Oversight of the Department of Justice: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (Nov. 18, 2009) (Statement of Eric Holder, Att’y Gen.) (LexisNexis Congressional).
down, and get into the weeds, and understand the details of our counterterrorism tools.

And that leads me to what I think are the right questions for today’s debate. As compared to the viable alternatives, what is the value of law enforcement in this war? Does it in fact help us win? Or is it categorically the wrong tool for the job – at best a distraction, and at worst an affirmative impediment?

III. LAW ENFORCEMENT IS AN EFFECTIVE COUNTERTERRORISM TOOL

Law enforcement helps us win this war. And I want to make clear, for the limited purpose of this article and in light of the nature of our current national debate, that this is not primarily a values-based argument. That is, I am not saying law enforcement helps us win in the sense that it is a shining city on a hill that captures hearts and minds around the world (although I do think our criminal justice system is widely respected). Values are critically important, both intrinsically and in terms of their effect on us, our allies, and our adversaries – and I will have more to say about values later – but right now, in part because of the nature of our national debate on this topic, I am talking about something more direct and concrete.

When I say that law enforcement helps us win this war, I mean that it helps us disrupt, defeat, dismantle, and destroy our adversaries (without destroying us or our way of life in the process). In particular, law enforcement helps us in at least three ways – it disrupts terrorist plots through arrests, incapacitates terrorists through incarceration after prosecution, and it can be used to obtain intelligence from terrorists or their supporters through interrogation, and through recruiting them as cooperating assets. Some of the evidence for that conclusion is set out below.

45. See infra Part III.C.

46. I describe several specific examples of intelligence obtained through the criminal justice system provided by the FBI and career prosecutors in NSD’s Counterterrorism Section in Appendix I. All the examples have been cleared for release by the FBI. They are by no means a comprehensive account of the breadth of intelligence that has been obtained through the criminal justice system. For a variety of reasons explained in greater detail in the appendix, including the need to protect the safety of sources and their families, as well as to protect ongoing operations, the FBI and other intelligence agencies are extremely cautious about making public the results of their intelligence collection efforts. The examples that are contained in Appendix I are included there only after extensive and careful review by the FBI to ensure that they could be made public.
A. Disruption, Incapacitation, Intelligence Collection

Since 9/11, the DOJ has convicted hundreds of defendants as a result of terrorism-related investigations. Some of these convictions have involved per se terrorism offenses, while others have not. Many of the terrorism

47. Here are 10 illustrative cases involving per se terrorism offenses, all from either the Southern District of New York or the Eastern District of Virginia:

- **U.S. v. Oussama Kassir.** Kassir was found guilty at trial of providing material support to al Qaeda, and other terrorism charges, for his efforts to establish a jihad training camp in the United States, and operate several terrorist websites. He was sentenced to life imprisonment on September 15, 2009.

- **U.S. v. Ahmed Omar Abu Ali.** Abu Ali was found guilty at trial of multiple terrorism charges based on his participation in an al Qaeda plot in Saudi Arabia to commit terrorist offenses in the United States, including a plot to assassinate the President. He was sentenced to life imprisonment on July 27, 2009.

- **U.S. v. Monzer al Kassar.** Kassar was found guilty at trial of conspiring to kill U.S. nationals and providing material support to the FARC in Colombia. He was sentenced to 30 years' imprisonment on February 24, 2009.

- **U.S. v. Mohammed Mansur Jabarah.** Jabarah pleaded guilty to terrorism charges stemming from his participation in a plot to bomb United States embassies in Singapore and the Philippines. He was sentenced to life imprisonment on January 18, 2008.

- **U.S. v. Ahmed Abdel Salat.** Salat, who was associated with Sheikh Abdel-Rahman and the Islamic Group, was found guilty at trial of conspiring to kill persons outside the United States. He was sentenced to 288 months' imprisonment on October 16, 2006.

- **U.S. v. Zaceirine Mousaoui.** Mousaoui pleaded guilty to participation in the 9/11 conspiracy and admitted receiving funds and support from the 9/11 defendants. He was sentenced to life imprisonment on May 4, 2006.

- **U.S. v. Menaad Khan.** Khan was a “Virginia Jihad” defendant convicted of waging war against the United States and providing material support to Lashkar-e-Taiba. Other defendants in the Virginia Jihad case were sentenced to terms of imprisonment of 65 years, 20 years, 17 years, and 15 years; Khan was sentenced to life imprisonment on June 15, 2004.

- **U.S. v. Lyman Faris.** Faris pleaded guilty to casing a New York City bridge for al Qaeda, and researching and providing information to al Qaeda regarding possible attacks on U.S. targets. He was sentenced to 20 years' imprisonment on October 28, 2003.

- **U.S. v. John Walker Lindh.** Lindh pleaded guilty to bearing arms in support of the Taliban and admitted that he had been trained in an al Qaeda training camp in Afghanistan. He was sentenced to 20 years' imprisonment on October 4, 2002.

- **U.S. v. Mokhtar Haouari.** Haouari pleaded guilty to participating in a plot to bomb the Los Angeles International Airport during millennium celebrations in 1999. He was sentenced to 288 months' imprisonment on January 16, 2002.

48. Here are six illustrative cases that do not involve per se terrorism offenses:

- **Fort Dix Plot (conspiracy to murder members of the U.S. military).** In 2008, Ibrahim Shnewer, Dritan Duka, Shain Duka, Eljvir Duka, and Serdar Tatar were convicted for their involvement in a plot to kill members of the U.S. military as well as for violating various weapons statutes. The government’s
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

convictions obtained in federal court both before and after 9/11 have

evidence revealed that one member of the group conducted surveillance at
several military bases in the United States, and that the group obtained a
detailed map of Fort Dix, where they hoped to use assault rifles to kill as many
soldiers as possible. The defendants performed small-arms training at a
shooting range in the Poconos and watched training videos depicting American
soldiers being killed and Islamic radicals urging jihad against the United
States. Ibrahim Shnewer, Dritan Duka, and Shain Duka were each sentenced
to life imprisonment plus thirty years; Elvir Durka was sentenced to life
imprisonment; and Serdar Tatar was sentenced to 33 years' imprisonment.

- **U.S. v. Sabri Benkahla** (perjury, obstruction, false statements). In 2007,
  Benkahla was convicted of perjury before a grand jury, obstructing justice, and
  making false statements to the FBI. These false statements included denial of
  his involvement with an overseas jihad training camp in 1999, as well as his
  asserted lack of knowledge about terrorists with whom he was in contact,
  including Ibrahim Bnsir of Ireland, and Manaf Kasmuri of Malaysia, both of
  whom are Specially Designated Global Terrorists. He was sentenced to 121
  months' imprisonment on July 24, 2007.

- **U.S. v. Mohammad Salman Farouq Qureshi** (false statements). In 2005,
  Qureshi was convicted of making of false statements to the FBI regarding the
  nature and extent of his involvement with al Qaeda member Wadhi E. Hage,
  and Help Africa People, a non-governmental organization believed to have
  been used to provide cover identities and funds in connection with the 1998
  attacks on the United States Embassies in Kenya and Tanzania. He was
  sentenced to 48 months' imprisonment on August 25, 2005.

- **U.S. v. Solomon Bibiiri** (false statements and passport fraud). In 2003 and
  2004, Solomon Bibiiri was convicted of fraudulently procuring a passport, as
  well as making false statements to federal agents. The government's evidence
  showed that Bibiiri had deliberately deceived federal agents during a June
  2003 interview in which he denied having business or personal ties to
  Mousa Abu Marzook, a Specially Designated Global Terrorist and a leader of
  Hamas. In fact, the government's evidence showed that Bibiiri had managed millions
  of dollars for Marzook both before and after Marzook was designated as a
  terrorist. He was sentenced to 13 months' imprisonment on January 14, 2005.

- **U.S. v. Fawaz Damrah** (citizenship fraud). In 2004, Fawaz Damrah was
  convicted of concealing material facts in his citizenship application. The
  government's evidence showed that in that application, Damrah concealed his
  membership in or affiliation with the Palestinian Islamic Jihad (PIJ) and his
  inclination of violent terrorist attacks against Jews and others. He was
  sentenced to two months' incarceration plus four months' house arrest and
  deportation on September 20, 2004.

- **U.S. v. Akram Musa Abdullah** (false statements). In 2009, Abdullah was
  convicted of making false statements to the FBI. These false statements were
  made during an interview in connection with an FBI investigation into the
  Holy Land Foundation for Relief and Development (HLF), which was pending
  trial at the time in federal court for crimes including providing material support
  to a foreign terrorist organization. During the interview, Abdullah denied
  involvement in numerous fundraising activities on behalf of HLF. In
  November 2008, HLF and seven of its principals were convicted on all
  charges. Abdullah was sentenced to 18 months' imprisonment on March 4,
  2010.
resulted in long sentences, including the convictions of the first World Trade Center bomber, Ramzi Yousef, and the East Africa Embassy bombers, Richard Reid, Ahmed Omar Abu Ali, Masaud Khan, Zacarias Moussaoui, and Oussama Kassir, all of whom are now serving life sentences in federal prison.

Today, law enforcement efforts against terrorism continue. In 2009, as outside observers have remarked, the DOJ charged more individuals with significant terrorism-related offenses than in any year since 9/11. This trend continued in 2010. Here are a few examples of recent terrorism charges or convictions: In June and August 2009, Syed Ahmed Harris and Ehsanul Islam Sadequee were each convicted in the Northern District of Georgia for providing material support to al Qaeda, including videotaping potential U.S. targets. They were sentenced to 13 and 17 years in prison, respectively.

In September 2009, Michael C. Finton was arrested and charged with terrorism offenses after he attempted to detonate an explosive device outside a federal building in Springfield, Illinois. That same month, Hosam Maher Husein Smadi was arrested and charged with attempting to detonate an explosive device outside an office building in Dallas, Texas. Smadi pleaded guilty in May 2010 to attempting to use a weapon of mass destruction, and he was sentenced in October 2010 to 24 years in prison. Finton is awaiting trial.

Also in September 2009, Najibullah Zazi was arrested just before carrying out a very serious plot to bomb the New York subway system; he pleaded guilty in February 2010 and is awaiting sentencing in the Eastern District of New York.

In October and December 2009, David Coleman Headley and Tahawwur Hussain Rana were charged in the Northern District of Illinois with conspiracy to attack a Dutch cartoonist overseas, and with assisting the terror attack in Mumbai, India that killed 164 people. Headley pleaded guilty in March 2010 to a dozen federal terrorism charges, admitting that he participated in planning both attacks, and he is awaiting sentencing; Rana is awaiting trial.

In May 2010, Faisal Shahzad was arrested in the Southern District of New York in connection with an attempted car bombing in Times Square; he pleaded guilty in June 2010 to all counts of the 10-count indictment against him, including conspiring and attempting to use a weapon of mass destruction, conspiring and attempting to commit an act of terrorism transcending national boundaries, attempting to use a destructive device during and in relation to a conspiracy to commit an act of terrorism

49. See Devlin Barrett, 2009 Was Big Year of Terror Charges in U.S., PITTSBURG POST-GAZETTE, Jan. 17, 2010, at A1. Of course, in many of these cases, the charges have not been proven, and defendants enjoy a presumption of innocence unless and until proven guilty.
transcending national boundaries, and transporting an explosive, among other charges. In October 2010, Shahzad was sentenced to life imprisonment.

In October 2010, James Cromitie, David Williams, Outa Williams, and LaGuerre Pen were convicted in the Southern District of New York after a jury trial for their participation in a plot to bomb a synagogue and Jewish community center and to shoot military planes with Stinger surface-to-air guided missiles. Each faces a mandatory minimum sentence of 25 years and maximum of life imprisonment.

The examples go on to include Mohammed Warsame, the Minnesota al-Shabaab cases, and Colleen LaRose ("Jihad Jane"), among others.

---


51. Here are some of the other notable cases involving defendants who were charged or convicted in 2009 or 2010:

* January 2009 — Zubair Ahmed and Khaled Ahmed (Northern District of Ohio): Cousins from Chicago pleaded guilty to conspiring to travel overseas to fight U.S. forces in either Iraq or Afghanistan. Zubair Ahmed was sentenced to ten years’ imprisonment and Khaled Ahmed to eight years’ imprisonment.

* April 2009 — Ali al-Marri (Central District of Illinois): Pleaded guilty to providing material support to al Qaeda. He was sentenced to 100 months’ imprisonment.

* May 2009 — Mohammed Abdullan Warsame (District of Minnesota): Canadian of Somali descent who trained with al Qaeda in Afghanistan in 2000. Pleaded guilty to providing material support to al Qaeda. He was sentenced to 92 months’ imprisonment.

* July 2009 — Daniel Patrick Boyd (Eastern District of North Carolina): U.S. citizen, charged with seven others in connection with various activities in support of violent jihad abroad. In February 2011, Boyd pleaded guilty to conspiracy to provide material support to terrorists and conspiracy to murder, kidnap, maim, and injure persons in a foreign country and is awaiting sentencing.

* September 2009 — Abdul Tawafa Ibn Ali Alishtai (Southern District of New York): Plead guilty to providing funding for terrorist training camps in Afghanistan. He was sentenced to 121 months’ imprisonment.

* November 2009 — Eight individuals linked to al Shabaab (District of Minnesota): Among fourteen men charged as part of ongoing investigation into the recruitment of persons from U.S. communities to train with or fight on behalf of extremist groups in Somalia.

* December 2009 — Omar Farouk Abdulmutallab (Eastern District of Michigan): Arrested and charged with terrorism offenses after he attempted to bring down Northwest Airlines flight 253 on Christmas day.

* January 2010 — Afia Siddiqui (Southern District of New York): Found guilty of attempt to murder U.S. personnel in Afghanistan. In September 2010, Siddiqui was sentenced to 86 years’ imprisonment.

* January 2010 — Zarein Ahmedzay and Adis Medunjanin (Eastern District of New York): Arrested and charged as part of ongoing investigation of
Not all of these cases made the headlines and not all of the defendants were hard-core terrorists or key terrorist operatives. The results of the cases vary according to several factors. First, as in traditional intelligence or criminal investigations, aggressive and wide-ranging counterterrorism efforts may net many small fish along with the big ones. Those small fish need to be dealt with, but – if they are indeed small fish – the charges will not necessarily yield the heavy penalties that accompany more serious offenses.52 In some of these cases, moreover, a conviction will support

Najibullah Zazi and others to attack New York subway system in September 2009. Ahmedzay pleaded guilty in April 2010 and is awaiting sentencing.

- March 2010 – Colleen LaRose (Eastern District of Pennsylvania): U.S. citizen arrested and charged with conspiring to murder a Dutch cartoonist and recruit jihadist fighters. LaRose pleaded guilty in February 2011 and is awaiting sentencing.

- May 2010 – Adnan Mirza (Southern District of Texas): Found guilty of conspiring to provide material support to the Taliban and unlawful possession of a firearm. He was sentenced to 15 years’ imprisonment in October 2010.

- June 2010 – Barry Walter Bujol (Southern District of Texas): U.S. citizen arrested and charged with attempting to provide material support to Al Qaeda in the Arabian Peninsula.


- June 2010 – Hor Akl and Amara Akl (Northern District of Ohio): Dual citizens of the United States and Lebanon arrested and charged with conspiring to provide material support to Hizbollah, a designated foreign terrorist organization.

- July 2010 – Madhata Asagai Haibe (District of Columbia): Philippines citizen and founding member of Abu Sayaff Group, a Philippines-based Islamist separatist group, pleaded guilty to hostage taking in connection with the 1995 abduction of 16 people, including four U.S. citizens in the Philippines. He was sentenced to 23 years imprisonment in December 2010.

- August 2010 – Ruselle DeFreitas, Abdul Khadir, Abdul Nur, Kareem Ibrahim (Eastern District of New York): DeFreitas and Khadir were convicted by a jury of plotting to blow up fuel tanks at John F. Kennedy International Airport. Khadir was sentenced to life imprisonment in December 2010. Nur pleaded guilty in June 2010 to his involvement in the plot and was sentenced to 15 years’ imprisonment in January 2011. DeFreitas is awaiting sentencing and Ibrahim is awaiting trial.


52. See U.S. DEP’T OF JUSTICE, UNITED STATES ATTORNEYS’ MANUAL §9.27.300 (2007) (“[A] Federal prosecutor should initially charge the most serious, readily provable offense or offenses consistent with the defendant’s conduct. Charges should not be filed simply to exert leverage to induce a plea, nor should charges be abandoned in an effort to arrive at a bargain that fails to reflect the seriousness of the defendant’s conduct.”).
deportation (and a plea agreement may support rapid deportation), which can mitigate threats posed to the homeland.  

Alternatively, there are cases in which a seemingly small fish may in fact be a big one, yet it may not be feasible either to prove that he is, or to establish an alternative basis for detaining him, even under the law of war. These cases pose the traditional tension between the intelligence benefit of continued surveillance and the risk to public safety from leaving a suspected terrorist at large (in other words, a tension between the values of short-term disruption and long-term incapacitation). In some of these cases, the risk-benefit equation will demand immediate action, disrupting a terrorist plot through arrest and prosecution for whatever criminal conduct can be established. Sometimes, a sentence of even a few months or years can shatter a terrorist cell and cripple its operational ability.

Finally, of course, disruptive arrests may also generate valuable intelligence. Some small fish may be ripe for recruitment precisely because they are not fully radicalized. Such persons may be persuaded to cooperate, either before or after they are released. Moreover, arrests and other disruptive efforts may provoke statements or actions from others that provide an understanding of a terrorist network — such cases effectively "shake the tree" and show how suspects still at large respond to the arrest.

Since 2001, in fact, the criminal justice system has collected valuable intelligence about a host of terrorist activities. In effect, it has worked as what the Intelligence Community would call a HUMINT collection platform.  

I will first explain how the system works as an intelligence collection platform — beginning with pre-arrest activity and ending with sentencing and beyond — and then turn to a few illustrative examples.

Pre-Arrest. Information can be obtained from the target of a criminal investigation or prosecution in a variety of ways. At the outset, in some investigations, the government may approach targets to assess their

53. Cf. Padilla v. Kentucky, 130 S. Ct. 1475, 1481 (2010) ("We have long recognized that deportation is a particularly severe 'penalty' . . . . Although removal proceedings are civil in nature, deportation is nevertheless intimately related to the criminal process. Our law has enmeshed criminal convictions and the penalty of deportation for nearly a century. And, importantly, recent changes in our immigration law have made removal nearly an automatic result for a broad class of noncitizen offenders. Thus, we find it 'most difficult' to divorce the penalty from the conviction in the deportation context." (citations omitted)). A recent example of deportation being used in the context of a criminal case, albeit one involving counterintelligence rather than counterterrorism, involves the Russian "illegal" agents who were arrested, pleaded guilty, were sentenced, and deported within a period of 12 days. See, e.g., Peter Baker & Benjamin Weiser, Russian Spy Suspects Plead Guilty as Part of a Swap, N.Y. TIMES, July 9, 2010, available at http://www.nytimes.com/2010/07/09/world/europe/09russia.html?_r=1&ref=russian_spy_ring_2010 (Westlaw).

54. "HUMINT," or "Human Intelligence," means intelligence obtained from human sources — as opposed to, for example, "SIGINT," or intelligence obtained from communications signals.
willingness to be interviewed prior to arrest. Typically, such targets are in a non-custodial setting and have agreed to be voluntarily debriefed. (In some ways, this is not very different from human source recruitment efforts conducted by other elements of the Intelligence Community.) These debriefings may last hours, days, or weeks and may result in the targets later agreeing to plead guilty and continue cooperating. In other cases, targets may talk for a while and then cease cooperating (if sufficient evidence exists, they then can be charged, arrested, prosecuted, and convicted.). In this kind of situation, targets cooperate (or do not cooperate) within the criminal justice system much as they do (or do not) outside of the criminal justice system.\(^{55}\)

**Arrest.** An arrest provides the next opportunity to gain intelligence from a target. At the time of arrest inside the United States, the FBI’s long-standing and publicly known policy, reaffirmed most recently in 2008,\(^{56}\) is generally to advise a target of his rights under *Miranda* prior to custodial interrogation except to the extent that the public-safety exception applies.\(^{57}\)

\(^{55}\) Although my primary focus here is on how law enforcement facilitates the collection of intelligence directly from human sources through such debriefings, there are of course a number of other ways in which law enforcement can and does obtain information that can be critical to counterterrorism efforts. These include, *inter alia*, FISA surveillance and searches; grand jury subpoenas, *see, e.g.*, United States v. Calandra, 414 U.S. 338, 343 (1974) ("The grand jury may compel the production of evidence or the testimony of witnesses as it considers appropriate, and its operation generally is unrestrained by the technical procedural and evidentiary rules governing the conduct of criminal trials."); Title III wiretaps, *see* 18 U.S.C. §§2510-22 (2006); the use of pen registers and trap and trace devices, *see* 18 U.S.C. §§3121-3127 (2006); and undercover operations, physical surveillance, and searches (with or without warrants), *see, e.g.*, Schneckloth v. Bostamonte, 412 U.S. 218, 219 (1973) (finding that a search conducted pursuant to consent is one of the specifically established exceptions to requiring a warrant and probable cause). Through these various methods, law enforcement can monitor electronic communications, review telephone records, obtain e-mails and other computer information, examine financial transactions, and collect a host of other documentary and electronic materials — sometimes in real-time and in secret — that can be instrumental in corroborating leads, identifying targets and their networks, and ensuring effective and comprehensive disruption of terrorist plots. The collection of such intelligence information through these other means also helps to make the debriefings of terrorist suspects themselves more productive. For a more thorough discussion of investigative tools available in the criminal justice system, see DAVID S. KIES & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS (2007).

\(^{56}\) The FBI’s current policy *vis-à-vis* *Miranda* warnings for arrests inside the United States is articulated in its 2008 Domestic Investigations and Operations Guide (DIOG), and in the Legal Handbook for Special Agents, the relevant portions of which have been in effect for many years. This policy, which is consistent with the policy of all U.S. law enforcement agencies, is to provide *Miranda* warnings prior to custodial interrogation. As the DIOG explains "[w]ithin the United States, *Miranda* warnings are required to be given prior to custodial interviews..." FBI DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 63 (2008). Of course, FBI policy also reminds agents that "standard booking questions and public safety questions" are not "interrogation" for purposes of *Miranda*. *Legal Handbook for Special Agents*, §7-2.1.1(1).

\(^{57}\) *Miranda v. Arizona*, 384 U.S. 436, 479 (1966) ("He must be warned prior to any [custodial] questioning that he has the right to remain silent, that anything he says can be
2011] LAw EnF orcemenT AS A CouNTerTerrorism Tool

The question whether a target will waive or invoke his Miranda rights, like the question whether or not he will respond to interrogation without such an advice of rights, depends on the facts and circumstances of a particular case, the disposition and training of the target himself, and the skill of the interrogators. It is difficult to know exactly what effect Miranda warnings have, because experiments with Mirandized interrogation would not easily allow for a control group of identical, un-Mirandized subjects, but the FBI’s experience over the years is that many arrestees waive their Miranda rights. 58 As FBI Director Mueller explained in a keynote speech at a conference sponsored by the Bipartisan Policy Center in October 2010, “I do believe that if you look at the number of recent cases we’ve had, Miranda has not stood in the way of getting extensive intelligence.” 59 And

used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires.”); see Florida v. Powell, 130 S. Ct. 1195 (2010) (upholding modified warnings as sufficient under Miranda); see also Dickerson v. United States, 530 U.S. 428 (2000) (holding that Miranda is a constitutional rule). There is an important exception for questioning focused on protecting public safety, which does not require Miranda warnings. See New York v. Quarles, 467 U.S. 649, 655-656 (1984); United States v. Khalil, 214 F.3d 111, 121 (2d Cir. 2000).

58. In one study, approximately 83% of suspects who were advised of their Miranda rights waived these rights. See Paul G. Cassell & Brett S. Hayman, Police Interrogation in the 1990s: An Empirical Study of the Effects of Miranda, 43 UCLA L. REV. 329, 861-71 (1996). While there is general agreement that the rate of waivers hovers in this range, scholars dispute the implications of this waiver rate. For example, one commentator has asserted that “the overwhelming majority of suspects (some 78-96%) waive their rights,” and that “Miranda warnings have little or no effect on a subject’s propensity to talk . . . .” Next to the warning label on cigarette packs, Miranda is the most widely ignored piece of advice in our society.” Richard A. Leo, Questioning the Relevance of Miranda in the 21st Century, 99 Mich. L. Rev. 1000, 1012-1015 (2001); see also George C. Thomas III, Stories About Miranda, 102 Mich. L. Rev. 1959, 1961-62, 1972, tbl.2 (2004) (finding waivers in 68% of a sample of appellate cases, which would not include most cases in which defendants waive their rights, cooperate, and plead guilty). On the other hand, while noting that the empirical research is limited, Cassell and Hayman conclude, based on studies done in the immediate wake of Miranda, that “confession rates fell substantially After Miranda.” Cassell & Hayman, 43 UCLA L. REV. at 846-849; see also Paul Cassell, Miranda’s Social Costs: An Empirical Reassessment, 90 NW. U. L. REV. 387, 417 (Winter 1996) (concluding that studies on the whole “report a drop in the confession rate after the Miranda decision, most in ‘double digits’”); Paul Cassell & Richard Fowles, Handcuffing the Cops? A Thirty-Year Perspective on Miranda’s Harmful Effects on Law Enforcement, 50 STAN. L. REV. 1055, 1061 (1998) (estimating Miranda’s social cost as the loss of convictions in 3.8% of all arrests). These conclusions have in turn been criticized for their methodology and assumptions. See, e.g., Donald A. Dripps, Constitutional Theory for Criminal Procedure: Dickerson, Miranda, and the Continuing Quest for Broad-But-Shallow, 43 WM. & MARY L. REV. 1, 54 n.276 (Oct. 2001) (criticizing assumptions underlying Cassell’s calculation of 3.8% conviction loss rate); Stephen J. Schulhofer, Miranda’s Practical Effect: Substantial Benefits and Vanishingly Small Social Costs, 90 NW. U. L. REV. 900, 301-307 (Winter 1996).

59. See Chris Strohm, FBI says Miranda Readings Don’t Hurt Bureau, CONGRESS
of those that do not waive their *Miranda* rights, of course, many might refuse to talk even without warnings. Some defendants do not talk initially, but after being given an opportunity to discuss their case with an attorney decide that cooperation is in their best interest. It is fair to say that *Miranda* warnings do not increase the likelihood of immediate cooperation, but it is also accurate to say that the extent to which they *decrease* that likelihood is vastly overstated in certain quarters. The FBI believes that the warnings are far less relevant to the prospects for obtaining long-term cooperation in the criminal justice system, even once defense lawyers have become involved, than other factors — such as the strength of the criminal case against the target, the interrogator’s skill and expertise, his ability to develop a rapport with the target, and his background knowledge about the target and the subject matter. I will have more to say about *Miranda* in Part V.

Presentment. Once an arrest is made, a target generally must be presented before a court without unnecessary delay, often within several hours, unless he waives the right to prompt presentment (which does sometimes occur).

60 At presentment, a Magistrate Judge typically advises the target that he is a criminal defendant, explains the charges against him, advises him that he has a right to a defense lawyer and to remain silent, and determines whether he should be detained or released pending trial. The period from presentment onwards may provide another opportunity for engaging with the target, especially in situations where he has already provided inculpatory information (such as through post-arrest statements).

Although it is not widely understood, the reality is that when sophisticated defense attorneys determine that the government has strong, admissible evidence to support a conviction and lengthy sentence, they will often encourage their clients to cooperate. In this sense, defense lawyers can be very helpful. They are obviously advocates for the target, and indeed they may earn the trust of the target precisely because of that; but they know that the criminal justice system is impregnable — its basic legitimacy and operation is beyond challenge — and that it has produced convictions in hundreds of thousands of cases. They know that where the federal government targets someone with a terrorism-related indictment, it almost always hits with a conviction, and that the system will grind forward and put their clients in prison for a long time. This creates powerful incentives to work within the system — to cooperate and obtain a somewhat

---


61. See **FED. R. CRIM. P. 5(d)**.
shorter sentence or improved conditions of confinement — rather than to challenge the system.\textsuperscript{62} (Of course, these incentives do not always work, and defense lawyers do not always counsel cooperation.)

Proffer and Plea. The criminal justice system has an established mechanism, known as a “proffer agreement,” under which a target and his lawyer may provide information to the government that cannot be used directly to prosecute the target, but can be used for its intelligence value or to investigate others.\textsuperscript{63} This often encourages candor from the target and provides the government with valuable, actionable intelligence at a relatively early stage. A successful proffer typically results in a guilty plea that requires further cooperation. A proffer agreement does not provide immunity from prosecution and almost always is made in connection with criminal charges that have already been filed.

Sentencing and Beyond. In rare situations, cooperation occurs after a conviction. Defense attorneys sometimes advise their clients to cooperate prior to sentencing so that they may receive a reduced sentence. Prosecutors may recommend that a cooperating target receive a downward departure from the otherwise applicable sentence pursuant to a provision of the U.S. Sentencing Guidelines.\textsuperscript{64} In a smaller class of cases, terrorist targets may even agree to cooperate after sentencing due to the incentives created by a Federal Rule of Criminal Procedure which allows the judge to re-sentence a prisoner to a shorter term based on a government motion citing his cooperation.\textsuperscript{65}

These mechanisms — the proffer agreement, and the pre- and post-sentencing cooperation provisions — allow the government to balance and re-balance over time the sometimes competing national security values of

\textsuperscript{62} Then Judge Michael Mukasey, in considering the habeas corpus petition of José Padilla, who had been declared an enemy combatant in 2002, expressly rejected the argument that granting Padilla access to counsel for the purposes of contesting the factual basis for his detention would necessarily “jeopardize the two core purposes of detaining enemy combatants — gathering intelligence about the enemy, and preventing the detainee from aiding in any further attacks against America.” Padilla v. Bush, 233 F. Supp. 2d 564, 603-605 (S.D.N.Y. 2002), reversed in part on other grounds, Padilla v. Rumsfeld, 332 F.3d 695 (2d Cir. 2003), reversed on other grounds, Rumsfeld v. Padilla, 542 U.S. 426 (2004).

Far from assuming that counsel would interfere with efforts to secure the detainee’s cooperation, Judge Mukasey found it “equally plausible” that if Padilla consulted with counsel, “the assured hopelessness of his situation would quickly become apparent to him ... and he might then seek to better his lot by cooperating with his captors.” Padilla v. Rumsfeld, 243 F. Supp. 2d 42, 52 (S.D.N.Y. 2003). He also referred to the “experience of federal courts under the U.S. Sentencing Guidelines” in arguing that “those facing the near certain prospect of custody have a fine appreciation of how to cut their losses.” Id. at n.7.

\textsuperscript{63} For a discussion of proffer agreements, see, e.g., United States v. Parra, 302 F. Supp. 2d 226 (S.D.N.Y. 2004).

\textsuperscript{64} United States Sentencing Guidelines §5K1.1; see 18 U.S.C. §3553(b) (2006); see also 9 USAM, CRIMINAL RESOURCE MANUAL at 792.

\textsuperscript{65} Fed. R. Crim. P. 35.
disrupting and incapacitating a particular target (through long-term incarceration resulting from successful prosecution based on admissible evidence) and gathering intelligence from the target that may help disrupt and incapacitate other terrorists (in exchange for a somewhat shorter period of incarceration). For example, depending on the facts, it may well be worthwhile to reduce a 50-year sentence to 40 years in exchange for actionable intelligence that allows the government – the Intelligence Community, the military, or the Justice Department – to neutralize one or more high-level terrorists in the short run.

The description just provided minimizes the use of legalese or law enforcement vocabulary. For example, the words “terrorism targets” rather than the word “defendants” appear. The purpose of minimizing legalese and law enforcement vocabulary is to describe the role of the criminal justice system as an intelligence collection platform, in terms that members of the Intelligence Community find familiar. When the FBI and prosecutors meet in a hotel room or an office with a criminal defendant and his lawyer, and talk to him for days or weeks in an effort to persuade him to plead guilty and cooperate, they can be described, and should be understood, as trying to collect human intelligence much as the CIA does when it tries to recruit human sources overseas. Of course, the processes differ, but both activities are aimed at the same purpose – the collection of human intelligence about the activities of terrorist groups. The different vocabulary of the criminal justice system should not obscure that shared purpose or the similarities in the information being generated.

Results. In terms of actual results, there is a limit to what can be said publicly (and to how what is said can be sourced), but I can say that terrorism suspects in the criminal justice system have provided information on all of the following:

- Telephone numbers and email addresses used by al Qaeda;
- Al Qaeda recruiting techniques, finances, and geographical reach;
- Terrorist tradecraft used to avoid detection in the West;
- Locations of al Qaeda training camps;
- Al Qaeda weapons programs and explosives training;
- Locations of al Qaeda safehouses (including maps);
- Residential locations of senior al Qaeda figures;
- Al Qaeda communications methods and security protocols;
- Identification of operatives involved in past and planned attacks; and
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

- Information about plots to attack U.S. targets.66

---

66. Here are some specific examples of intelligence obtained through the criminal justice system that have been provided by the FBI and career prosecutors in NSA's Counterterrorism Section:

- A terrorism suspect arrested in 2002 provided the FBI with information regarding the role of Khalid Sheikh Mohammed (KSM) as the principal architect of the 9/11 attacks, stated that KSM was continuing to plan terrorist plots against the United States, and provided the FBI with telephone numbers and e-mail addresses that he had used to contact KSM immediately prior to his arrest. The individual also told the FBI that KSM and Hamzah were directing their participation in a joint al Qaeda/Iqmaa Islamiyya plot to bomb U.S. military targets and U.S. and Israeli Embassies in Singapore. Although the plot had been disrupted prior to the individual's arrest, he identified other participants and provided contact information for them. This was especially significant because neither KSM nor Hamzah had been captured at the time.

- A terrorism suspect arrested in 2003 explained to the FBI that he had traveled to Afghanistan in March 2002 to train at an al Qaeda camp that he referred to as "the camp of Osama bin Laden." He advised the FBI that in addition to basic training, specialized training was carried out at the camp, including the use of anti-aircraft guns, explosives, suicide missions and poisons. He explained that other trainees in the camp were being taught how to attack locations by using poison gas. He also explained that he had met with Abu Hafs, then al Qaeda's military commander, who advised him of al Qaeda tactics that could be used to avoid suspicion when he traveled back to North America. The FBI believed that this individual had been dispatched by al Qaeda for an operation in the United States and that the operation was likely disrupted by his arrest and interviews.

- A terrorism suspect arrested in 2001 told the FBI that he met personally with Osama bin Laden at an al Qaeda poisons training facility near Kandahar, Afghanistan. He provided information about bin Laden, such as his appearance, since the September 11, 2001 attacks, bin Laden and his cadre of bodyguards moved every four hours to avoid capture, and a description of the vehicles used in bin Laden's convoy. He also explained that according to other al Qaeda members and training camp instructors, bin Laden had plans for additional attacks against the United States and had already dispatched operatives to carry out future attacks. This individual described in detail the training he had received from al Qaeda, the facilitators who aided his entry into training camps, and the camp instructors.

- A terrorism suspect provided information to the FBI on potential hide-outs of Osama bin Laden in Afghanistan. He drew detailed maps of specific locations which were provided to the DoD prior to the U.S. invasion of Afghanistan.

- A terrorism suspect told the FBI, in the course of multiple interviews in the spring of 2003 prior to his arrest, about al Qaeda operations, leaders, and plans for attacks to be conducted in the United States. He provided detailed information and identified photos of Masood Khan, a high-ranking al Qaeda associate who was involved with KSM and at the time was in Pakistan and being sought by the United States, including detailed descriptions of vehicles that Masood used to travel within Pakistan and his communication protocol and security measures. Using a map, he then identified the location of

---

203
The Intelligence Community, including the National Counterterrorism Center (NCTC), believes that the criminal justice system has provided useful information. For example, NCTC has explained that it “regularly receives and regularly uses . . . valuable terrorism information obtained through the criminal justice system — and in particular federal criminal proceedings pursued by the FBI and DOJ. Increasingly close coordination between the DOJ and NCTC has resulted in an increase in both the intelligence value and quality of reporting related to terrorism.”

In short, law enforcement is a strong counterterrorism tool. It can disrupt terrorist plots through arrests or other interventions. It can incapacitate terrorists for the long term through prosecution and conviction. And it can be used to obtain valuable intelligence that supports continuing efforts — including non-law enforcement efforts — against terrorism.

B. Counterarguments

Given the basic affirmative case for law enforcement as a counterterrorism tool, what are some of the arguments opposing its use?

The first argument is that there is an inherent tension between national security and law enforcement. This argument confuses ends with means. The criminal justice system is a tool — one of several — for promoting national security, for protecting our country against terrorism. Sometimes it

an al Qaeda safehouse and camp located near Kandahar, where he had previously met with Osama bin Laden. He also identified a photo of KSM and explained that he knew KSM by an alias, as a high ranking al Qaeda official whom he had met during his lunch with bin Laden; this was particularly significant because KSM had been captured only weeks before in Pakistan. He described meetings with KSM in which he was tasked to perform surveillance on specific targets in the United States, and noted that KSM was particularly interested in obtaining forged American drivers' licenses and social security cards for al Qaeda operatives so that they could enter the United States without suspicion. This individual also provided information to the FBI regarding links between KSM, Majood and other individuals sympathetic to al Qaeda located in the United States, including his contacts with Majid Khan, a high value detainee who had been arrested in Pakistan in the weeks prior to the individual's interview with the FBI.

- Appendix 1 further discusses these as well as some additional examples of intelligence on the activities of terrorist groups obtained through the criminal justice system. These examples have been cleared for release by the FBI. They are by no means a comprehensive account of the breadth of intelligence that has been obtained through the criminal justice system. For a variety of reasons explained in greater detail in the Appendix itself, including the need to protect the safety of sources and their families, as well as to protect ongoing operations, the FBI and other intelligence agencies are extremely cautious about making public the results of their intelligence collection efforts. The examples that are contained in Appendix 1 are included therein only after extensive and careful review by the FBI to ensure that they could be made public.
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

is the right tool; sometimes it is not, just as sometimes the best way to protect national security is through diplomacy, and sometimes that goal is better achieved through military action.

Another argument is that the criminal justice system is fundamentally incompatible with national security because it is focused on defendants' rights. This argument suffers from two basic flaws. First, the criminal justice system is not focused solely on defendants' rights — it strikes a balance between defendants' rights and the interests of government, victims, and society. And whatever that balance is in any given case, the empirical fact is that when we prosecute terrorists we convict them around 90 percent of the time. To be sure, the criminal justice system has its limits, and in part because of those limits it is not the right tool for every job. But when the executive branch concludes that it is the right tool — as it has many times since 9/11 — it in fact puts steel on target almost every time.

The second flaw in the "fundamental incompatibility" argument is equally significant. The criminal justice system is not alone in facing legal constraints. All of the U.S. government's activities must operate under the rule of law. For example, the U.S. military operates under rules that require it to forgo strikes against terrorists if the strikes will inflict disproportionate harm on civilians. It also has rules governing who may be detained, how

67. A Justice of the Supreme Court once famously observed that the reasonable-doubt standard used in the criminal justice system is bottomed on the determination that it is far worse to convict an innocent man than to let a guilty man go free. In re Winship, 397 U.S. 358, 372 (1970) (Harlan, J., concurring) ("I view the requirement of proof beyond a reasonable doubt as bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free.").

68. See, e.g., CTR. ON LAW AND SEC., N.Y. UNIV. LAW SCH., TERRORIST TRIAL REPORT CARD 4 (2010) (calculating that approximately 87% of terrorism prosecutions between September 11, 2001 and September 11, 2010 resulted in convictions, either after trial or after a guilty plea); Richard B. Zabel & James J. Benjamin, Jr., In Pursuit of Justice: Prosecuting Terrorism Cases in the Federal Courts, 2009 Update and Recent Developments 9 (2009) (calculating that over 91% of charges filed in terrorism prosecutions between September 12, 2001 and June 2, 2009, resulted in a conviction on some charge, whether after trial or after a guilty plea).

69. See, e.g., Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48-51, June 8, 1977, 1125 U.N.T.S. 3 (hereinafter Protocol I) (stating that civilians shall not be the object of attack, requiring parties to conflict to "at all times distinguish between the civilian population and combatants and between civilian objects and military objectives," and prohibiting "indiscriminate attacks," including those "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated") (signed but not ratified by the United States); Convention (IV) Respecting The Laws And Customs Of War On Land and Its Annex: Regulation Concerning the Law and Customs of War On Land arts. 22-28, 18 October 1907, 36 Stat. 2277 (regulating the "[n]eeds of injuring the enemy, sieges, and bombardments" including prohibitions on certain weapons; attacking undefended towns, villages, dwellings, or buildings; requiring "all necessary steps"
detainees have to be treated, and how long they can be held. These limits are real, and they are not trivial, but they are not a reason to abandon or forbid the use of military force against al Qaeda.

Some say that the criminal justice system should not be used to deal with terrorists because it treats them like common criminals, which they are not. (On the other hand, of course, others say that treating terrorists as combatants glorifies them as soldiers in a holy war and elevates them to a status they do not deserve.) For the pragmatist, however, the key question to spare artistic and historic buildings as well as hospitals) [hereinafter Hague IV]; U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE, ¶25 (Enmty Status of Civilians) ("[I]t is a generally recognized rule of international law that civilians must not be made the object of attack directed exclusively against them."). See also Hamdi v. Rumsfeld, 542 U.S. 507, 521 (2004).

70. See, e.g., Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 6 U.S.T. 3306 [hereinafter Fourth Geneva Convention]. The four Geneva Conventions govern, among other matters, the care and treatment of prisoners of war and the treatment of civilians during wartime; in particular, Common Article 3 of the Geneva Conventions, governing non-international armed conflicts, mandates minimum treatment standards for all detainees, and two additional protocols. Additional Protocols I and II, amplify the Geneva Conventions on issues such as the treatment of combatants and civilians during international and non-international armed conflicts respectively. The United States is a party to all four Geneva Conventions and is a signatory to, but has not ratified, the two additional protocols. See also U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, ¶50-207 (mandating regulations for prisoners of war); DEP'T OF DEF. DIRECTIVE 2310.01E (Department of Defense Detainee Program) (regulating treatment of detainees, mandating humane treatment, and stating that all persons subject to it must apply at a minimum the standards articulated in Common Article 3), available at http://www.dtic.mil/whs/directives/corrers/pdf/231001p.pdf.

71. The point of this argument is not to equate the legal constraints in the two systems; they are in fact very different. The point is only to emphasize that all of our counterterrorism tools have legal limits—this is the price of living under the rule of law—and those limits inform judgments about which tool is best in any given case.

72. In imposing a life sentencing on Richard Reid, Judge William Young provided the following explanation:

This is the sentence that is provided for by our statutes. It is a fair and a just sentence. It is a righteous sentence. Let me explain this to you. We are not afraid of any of your terrorist co-conspirators, Mr. Reid. We are Americans. We have been through the fire before. There is all too much war talk here. And I say that to everyone with the utmost respect. . . . You are not an enemy combatant. You are a terrorist. You are not a soldier in any war. You are a terrorist. To give you that reference, to call you a soldier gives you far too much stature. . . . And we do not negotiate with terrorists. We do not treat with terrorists. We do not sign documents with terrorists. We hunt them down one by one and bring them to justice. . . . You’re no warrior. I know warriors. You are a terrorist. A species of criminal guilty of multiple attempted murders. Look around this courtroom. Mark it well. The world is not going to long remember what you or I say here. Day after tomorrow it will be forgotten. But this, however, will long endure. Here, in this courtroom, and courtrooms all across America, the American people will gather to see that justice, individual justice, justice, not war, individual justice is in fact being done.

Judgment and Conviction and Statement of Reasons for Sentence at 5-6 United States v.
is not about labels per se, it is about whether the treatment of terrorists is effective (and consistent with our laws and values). The argument that somehow it is inherently “wrong” (strategically) to treat terrorists as criminals is problematic because it provides a theoretical and aesthetic answer to what is, or should be, an empirical and operational question.

Consider the “common criminals” argument as applied to the hypothetical case of a young man apprehended in the course of an attempted terrorist attack in the United States. Assume for purposes of discussion that one possibility may be to hold him under the law of war—he can be transferred to the custody of uniformed military personnel, detained without charges at a brig, and interrogated under the Army Field Manual.73 There is a certain appeal to this approach because it is very forceful. But what if the Intelligence Community interrogators who have had direct contact with the young man, and their colleagues who have searched our databases for everything known about him, have a different view? What if they believe that transferring him to military custody will only fuel his belief that he is a holy warrior engaged in a noble, armed conflict against a powerful adversary, thus galvanizing his resistance to interrogation? What if they believe that the best thing is to hold him in civilian custody and invite his family to visit in an effort to persuade him to cooperate? For the pragmatist, this is an easy call: If a visit from his family is the best way to get him to talk, then he should have a visit from his family. This approach may provoke questions about why the terrorist is being treated like a common criminal, or otherwise being “coddled,” but if it actually works it is clearly preferable.

C. Pragmatism and Perception

Rejecting the “common criminals” argument, of course, does not necessarily reject the idea that perception matters. Treating terrorists one way or another, and describing our treatment of them in one way or another, does send a message to our own people and to the people of other countries, which in turn may trigger responses with real-world effects. In advocating a pragmatic approach to counterterrorism, I have so far focused on particular matters and cases, assessing the effectiveness of our tools in that relatively narrow context (albeit with reference to nearly a decade’s worth of statistical data and experience). I have done so because I think a granular approach is valuable—indeed, indispensable—and also because I worry that it is underrepresented in our current policy debate. But I do not

Richard Colvin Reid, No. 02 Cr. 10013-WGY (Jan. 31, 2003).

73. The legal authority for this detention with respect to individuals found in the United States is not yet settled, see infra notes 137 and 147, but that is irrelevant to the present discussion.
want to completely lose sight of the larger landscape, even if I continue to view it from a pragmatic perspective.

First, with respect to our own people, in advocating a pragmatic approach, we need to be on guard against operational bias. This means that those who work in the criminal justice system sometimes need to be reminded that the system is not the only answer to the terrorist threat. When law enforcement personnel encounter a terrorist, or someone who may know something about terrorism, they need to recognize that prosecution is not an end in itself. It is a means to an end. Law enforcement personnel must use all available tools to collect the intelligence needed to protect the country. They must see themselves as part of a larger effort. If they become too parochial, they will miss opportunities to protect national security. For example, I mentioned before 74 that where a problem looks like a nail we need to use a hammer and where it looks like a bolt we need to use a wrench. A related point is worth making here: To a person whose job is to use a hammer, every problem can begin to look like a nail. The Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, has spoken recently on the importance of seeing military power in the context of U.S. national interests as a whole. 75 and law enforcement power should be viewed in that way as well. If, as will often be the case under present conditions, law enforcement agents are the first to encounter terrorists in the United States, those agents must be careful to act in accord with our overall national interest. They should not tightly take actions that foreclose other methods consistent with our values that may be more effective for achieving our goals.

On the other side of the balance, certainly most of our friends in Europe, and indeed in many countries around the world (as well as many people in this country), accept only a law enforcement response and reject a military response to terrorism, at least outside of theaters of active armed conflict. 76 As a result, some of those countries will restrict their cooperation with us unless we are using law enforcement methods. Gaining cooperation from other countries can help us win the war – these countries can share intelligence, provide witnesses and evidence, and transfer terrorists to us. Where a foreign country will not give us a terrorist (or information needed to neutralize a terrorist) for anything but a criminal prosecution, we obviously should pursue the prosecution rather than letting the terrorist go free. This does not subordinate U.S. national interest to some global test of

74. See supra Part II.


76. As discussed in Part I, supra, the Obama administration has made clear that it will use military commissions and law of war detention. See infra Part IV.
legitimacy; it simply reflects a pragmatic approach to winning the war. If we want the help of our allies, we need to work with them.  

More generally, we need to recognize the practical impact of our treatment of the enemy and the perception of that treatment. This war is not a classic battle over land or resources, but is fundamentally a conflict of values and ways of life.  

Demonstrating that we live up to our values, thus drawing stark contrasts with the adversary, is essential to ensuring victory. When our enemy is seen in its true colors – lawless, ruthless, merciless – it loses support worldwide. For example, in Iraq, al Qaeda’s random and widespread violence against civilians eventually helped mobilize the population against the insurgents. On the other hand, when our actions or policies provoke questions about whether we are committed to the rule of law and our other values, we risk losing some of our moral authority. This makes it harder to gain cooperation from our allies and easier for the terrorists to find new recruits.

This is not simply abstract philosophy. It is an important reality in our military’s effort to defeat the enemy in places like Iraq and Afghanistan. As the U.S. military’s counterinsurgency field manual states, “to establish legitimacy, commanders transition security activities from combat operations to law enforcement as quickly as feasible. When insurgents are seen as criminals, they lose public support.”

Adherence to the rule of law

---

77. I will have more to say about international cooperation issues as part of the comparison between the criminal justice system, the system of reformed military commissions, and law of war detention.

78. The Department of Defense’s 2008 National Defense Strategy report provides: “This conflict is a prolonged irregular campaign, a violent struggle for legitimacy and influence over the population. The use of force plays a role, yet military efforts to capture or kill terrorists are likely to be subordinate to measures to promote local participation in government and economic programs to spur development, as well as efforts to understand and address the grievances that often lie at the heart of insurgencies. For these reasons, arguably the most important military component of the struggle against violent extremists is not the fighting we do ourselves, but how well we help prepare our partners to defend and govern themselves.” DEPT OF DEF., NATIONAL DEFENSE STRATEGY (June 2008) at 8, available at http://www.defense.gov/pubs/2008NationalDefenseStrategy.pdf.

79. See, for example, General David Petraeus’s speech at the Marine Corps Association Dinner in July 2009, in which he described the complex of factors that led to the so-called “Anbar Awakening” – the effort there required both fierce fighting and building trust with local partners, including protecting allies and “also required living among, and sharing the risks with, those whose trust we sought; training, equipping, and funding security forces capable of protecting their own neighborhoods; and, once an area had been cleared of insurgents, doing the hard work of rebuilding not only local infrastructure, but also local governance and rule of law. . . . Eventually, we reached a tipping point. The Coalition demonstrated its ability to protect the population and its long-term commitment to the fight, and insurgent attacks started to drive more Anbaris to our side.” The speech is available at http://www.cenicom.mil/en/from-the-commander/commanders-speech-to-marin-corpsassociation-annual-dinner.html.

is central to this approach: "The presence of the rule of law is a major factor in assuring voluntary acceptance of a government's authority and therefore its legitimacy. A government's respect for preexisting and impersonal legal rules can provide the key to gaining widespread enduring societal support. Such respect for rules - ideally ones recorded in a constitution and in laws adopted through a credible, democratic process - is the essence of the rule of law. As such, it is a powerful potential tool for counterinsurgents." Indeed, the U.S. military has been implementing such a transition to civilian law enforcement in Iraq, where detentions and prosecutions of insurgents are now principally processed through the domestic criminal justice system, and we are moving in that direction in Afghanistan, where transfer of detention and prosecution responsibilities to Afghan civilian authorities is our goal. I think these are principles that are well worth keeping in

2006).

81. Id. at §1-119.

82. U.S. detention operations in Iraq are governed by the Agreement Between the United States of America and the Republic of Iraq On the Withdrawal of United States Forces from Iraq and the Organization of Their Activities during Their Temporary Presence in Iraq, Nov. 17, 2008, (available at http://www.usf-iraq.com/images/CGs_Messages/security_agreement.pdf) (hereinafter Security Agreement). The Agreement entered into force on January 1, 2009, and governs the U.S. military presence in Iraq. The Agreement addresses both disposition of legacy security detainees, who were detained pursuant to the United Nations mandate for the Multi-National Force-Iraq prior to January 1, 2009, and new captures. Security Agreement, at art. 22. Under the Agreement, legacy security detainees whom Iraqi authorities wish to prosecute are transferred to the Government of Iraq upon presentation of a valid criminal arrest warrant and detention order. Id. at art. 22(4). Detainees against whom a criminal case is not brought must be released by U.S. forces "in a safe and orderly manner, unless otherwise requested by the Government of Iraq and in accordance with Article 4 of this Agreement." Id. A request by the Government of Iraq for another disposition might include repatriation to a third country. To mitigate security risks, U.S. forces release detainees whom Iraqi authorities have determined would not be prosecuted in order of least to greatest security threat. New captures are processed in line with the Iraqi judicial system. The Agreement precludes U.S. forces from arresting or detaining individuals "except through an Iraqi decision issued in accordance with Iraqi law and pursuant to Article 4" of the Agreement, which authorizes U.S. military operations and requires U.S. forces to respect Iraqi law. Id. at art. 22(1). The preference is to arrest an individual pursuant to an Iraqi-issued arrest warrant; if a warrant is not feasible, individuals taken into U.S. forces' custody must be turned over to a competent Iraqi authority within 24 hours, at which point Iraqi authorities determine whether continued detention is warranted. Id. at art. 22(2). The Agreement also affirms that U.S. forces in Iraq retain the right to legitimate self-defense. Id. at art. 4(3).

83. See, e.g., Gen. Stanley McChrystal, then Commander, Int'l Sec. Assistance Force (ISAF), Joint News Briefing with Ambassador Mark Sedwill, NATO Representative in Afghanistan (March 17, 2010) available at http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4589, ("The most important thing is we're in a major effort here to turn detainee operations over to Afghan control. Our JTF-435, under Vice Admiral Bob Harward, is working already in partnership. So through 2010, we will be in the lead, but they will be partnering with us at places like the detainee facility in Parwan, right outside of Bagram. And then we look to 1 January 2011, for it to be Afghan ownership. We think it's an important step in their sovereignty and their control of this entire effort. And we would
mind as we think about the impact of employing different tools in the context of our conflict with al Qaeda. It would not only be ironic, but also operationally counterproductive, if our partners in Iraq and Afghanistan rely increasingly on law enforcement tools to detain terrorists, even in areas of active hostilities, while we abandon those tools here in the United States.\textsuperscript{44}

IV. COMPARING THE CRIMINAL JUSTICE AND MILITARY DETENTION SYSTEMS

Ultimately, the value of the criminal justice system as a counterterrorism tool is relative. It must be compared to the value of other tools. Comparing the criminal justice system to the use of military force or diplomacy is difficult, because it has so little in common with them. But insofar as it permits us to disrupt and incapacitate terrorists, and to gather intelligence, the criminal justice system is readily comparable with two other systems – detention under the law of war, and prosecution in a military commission.\textsuperscript{45} I will now turn to these comparisons.

\textsuperscript{44} Of course, I am by no means suggesting that our military, when operating in Iraq or Afghanistan, or in any other military context, should employ law enforcement tools against our enemies – by, for example, providing \textit{Miranda} warnings to captured individuals or adopting other practices that would be inconsistent with its primary mission. The primary mission of our nation’s military is to capture or engage the enemy, not to collect evidence for criminal prosecutions. My point is that there is a very important role for domestic, civilian law enforcement even in places like Iraq and Afghanistan that are confronting large-scale insurgencies and where our military is actively engaged. I should add one additional and important note here. In most of the discussion, I have talked about values primarily as a threshold determination – we determine the tools that are consistent with our laws and values, and then we make them available to our operational personnel. As President Obama made clear in his speech at the National Archives, however, it can also be the case that our values tolerate the use of certain methods, but only as a last resort. \textit{See supra} 42. The President made that point with respect to long-term law of war detention for detainees held at Guantánamo Bay. I do not mean to discount this more nuanced approach to the role of values in determining the tools we should use to defeat our enemies in the current conflict.

\textsuperscript{45} Executive Order No. 13,356, \textit{Periodic Review of Individuals Detained at Guantánamo Bay Naval Station Pursuant to the Authorization for Use of Military Force,} 76 Fed. Reg. 13,277 (March 10, 2011) (directing a system of periodic review for persons detained at Guantánamo Bay). The order provides that “[a]s to each detainee whom the interagency review established by Executive Order 13492 has designated for continued law of war detention, the Attorney General and the Secretary of Defense shall continue to assess whether prosecution of the detainee is feasible and in the national security interests of the
Before I focus on the differences between these systems, however, I want to acknowledge the similarities of the two prosecution systems. Prosecution in an Article III federal court and prosecution before a military commission have many requirements and elements in common. These include the presumption of innocence and the requirement that guilt be proven beyond a reasonable doubt; the right to notice of the charges; the right to counsel and choice of counsel; the right to present evidence, cross-examine the government's witnesses, and compel the attendance of witnesses in one's defense; the right to exculpatory evidence that the prosecution may have as to guilt, sentencing and the credibility of

United States, and shall refer detainees for prosecution, as appropriate." In an accompanying press release, which is available at http://www.whitehouse.gov/the-press-office/2011/03/07/fact-sheet-new-actions-guant-namo-and-detainee-policy, the White House stated that "[t]he Secretary of Defense will issue an order rescinding his prior suspension on the swearing and referring of new charges in the military commissions."

86. Coffin v. United States, 156 U.S. 432, 453 (1895) (presumption of innocence); In re Winship, 397 U.S. at 364 (finding that due process requires prosecution to prove defendant guilty of each element beyond a reasonable doubt); 10 U.S.C. §949(2)(c)(1) (2006) (requiring that members be instructed that accused is presumed innocent until guilt is established beyond a reasonable doubt).

87. U.S. Const. amend. VI; Cook v. United States, 138 U.S. 157 (1891) (finding that the defendant is entitled to be informed of the nature of the charge with sufficiently reasonable certainty to allow for preparation of the defense); 10 U.S.C. §§48(8) (2006) (requiring assigned trial counsel to serve defense counsel copy of the charges in English and, if appropriate, another language "sufficiently in advance of trial to prepare a defense").

88. U.S. Const. amend. VI; United States v. Gonzalez-Lopez, 548 U.S. 140, 144 (2006) (finding that the Sixth Amendment right to counsel includes the right of a defendant who does not require appointed counsel to choose who will represent him); 10 U.S.C.A. §949(a)(2)(C)(i) (West 2009) (right to be represented by civilian counsel at no expense to the government and by either defense counsel detailed or the military counsel of the accused's own selection, if reasonably available).

89. Illinois v. Allen, 397 U.S. 337, 338 (1970) (finding that the Confrontation Clause of Sixth Amendment guarantees a defendant's right to be present at trial); id. at 343 ("a defendant can lose his right to be present at trial if, after he has been warned by the judge ... he nevertheless insists on conducting himself in a manner so disorderly, disruptive, and disrespectful of the court that his trial cannot be carried on with him in the courtroom."); 10 U.S.C.A. §949(a)(2)(B) (West 2009) (right to be present at all sessions of the military commission other than for deliberation or voting except as set forth in §949d); 10 U.S.C.A. §949(d)(1)-2 (West 2009) (military judge may exclude the accused upon a determination that, after warning, accused persists in conduct that justifies exclusion to ensure physical safety or prevent disruption).

90. U.S. Const. amend. VI; Bram v. United States, 168 U.S. 532, 542 (1897); 10 U.S.C.A. §948(b) (West 2009) ("No person shall be required to testify against himself or herself at a proceeding of a military commission ... ").

2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL 35

adverse witnesses, the right to an impartial decisionmaker, and similar
procedures for the selection of jurors and commission members, the right
to suppression of evidence that is not reliable or probative or that will result
in unfair prejudice, confusion, or be misleading to the jury/commission;
the right to qualified self-representation, protection against double

92. Brady v. Maryland, 373 U.S. 83, 87-88 (1963) (finding that the suppression by
prosecution of evidence favorable to accused violates due process where evidence is material
either to guilt or punishment); Giglio v. United States, 405 U.S. 150, 154 (1972) ("When the
"reliability of a given witness may well be determinative of guilt or innocence," nondisclosure of evidence affecting credibility "could justify a new trial."); 10 U.S.C.A.
§949(b)(b) (West 2009) (right to exclamatory evidence as to guilt, sentencing, and the
credibility of adverse witnesses).

93. In Article III criminal trials, the Sixth Amendment guarantees the criminal
defendant the right to be tried by an impartial jury. See Gray v. Mississippi, 441 U.S. 648, 658 (1987) ("The right to an impartial adjudicator, be it judge or jury" is "basic to a fair
trial."). In military commissions, attempting to influence the decision-making of military
trial judges, commission members, and appellate judges is prohibited, except for narrow
exceptions (which relate to the training of military judges and the provision of instructions to
convening a military commission . . . may censure, reprimand, or admonish the military
commission, or any member, military judge, or counsel thereof, with respect to the findings
or sentence . . . or with respect to any other exercises of its or their functions in the conduct
of the proceedings."); 10 U.S.C.A. §949(b)(2) (West 2009) ("No person may attempt to
coerce or, by any unauthorized means infringe the actions of a military commission or
commission members; convening, approving or reviewing authority "with respect to their
judicial acts" or "the exercise of professional judgment by trial counsel or defense
counsel."); 10 U.S.C.A. §949(b)(3) (West 2009) (similar provisions on appeal regarding the
U.S. Court of Military Commission Review (CMCR)). Of course, unlike in an Article III
criminal trial, all of the members of the commission, as well as the judges, must be military

94. See FED. R. CRIM. P. 24 (explaining voir dire process for selection of trial jurors);
U.S. DEP'T OF DEF., MANUAL FOR MILITARY COMMISSIONS (2010), Rule 912 (explaining voir
dire process for selection of military commission members including questionnaire and

95. See FED. R. EVID, 402 (relevant evidence generally admissible; irrelevant evidence
generally inadmissible), 403 (exclusion of evidence on grounds of unfair prejudice,
confusion of the issues, or waste of time); 10 U.S.C.A. §§949a(b)(2)(E) (West 2009)
(suppression of evidence that is not reliable or probative) and 949a(b)(2)(F) (West 2009)
(suppression of evidence on grounds of unfair prejudice, confusion of the issues or
misleading the members, or undue delay, waste of time, or cumulative nature of evidence).

96. Farella v. California, 422 U.S. 306, 821, 835 (1975) (finding that the Sixth
Amendment gives criminal defendant right to conduct own defense in a criminal case; to
proceed pro se, defendant must knowingly and intelligently waive right to counsel);
McKee v. Wiggins, 465 U.S. 168, 169 (1984) (holding that the Sixth Amendment is not
violated when trial judge appoints stand-by counsel, even over defendant's objection, in
order to ensure that defendant understands and follows "basic rules of courtroom protocol");
10 U.S.C.A. §949a(b)(2)(D) (West 2009) (right to self-representation if "accused knowingly
and competently waives assistance of counsel" and "conform[s] the accused's departure
and the conduct of the defense to the rules of evidence, procedure, and decorum applicable
to trials by military commission").
jeopardy;\textsuperscript{97} a prohibition on ex post facto laws;\textsuperscript{98} protections for incompetent defendants;\textsuperscript{99} and the right to an appeal;\textsuperscript{100} among others. The U.S. Constitution secures many of these rights in federal court, and may also secure these rights in the context of military commissions. The 2009 Military Commissions Act (2009 MCA or MCA)\textsuperscript{101} provides most of these basic procedural protections as a statutory matter.

It is also important to note that while the criminal justice and military prosecution systems share certain essential characteristics and also a common punitive function, the legal basis and rationale for law of war detention is fundamentally different. As a plurality of the Supreme Court explained in Hamdi, during a war or armed conflict, a state that captures enemy forces can lawfully hold them for the duration of the conflict.\textsuperscript{102} Unlike criminal prosecution, holding a detainee under the law of war is not penal in nature; a detainee is not convicted of a criminal act or subject to a criminal sentence. When hostilities end, international law requires prompt repatriation.\textsuperscript{103} Because the legal basis and rationale of law of war detention

\textsuperscript{97} U.S. CONST., amend. V; Price v. Georgia, 398 U.S. 323, 326 (1970); 10 U.S.C.A. §949h (West 2009) ("No person may, without the person's consent, be tried by a military commission . . . a second time for the same offense.").

\textsuperscript{98} U.S. CONST., art. I, §§; Miller v. Florida, 482 U.S. 423 (1987); United States v. Hamdan, 2 M.C. 1, 2 (2008) ("Congress is not authorized to pass ex post facto legislation.").


\textsuperscript{100} 28 U.S.C. §§1291-92 (2006) (federal appellate courts may review final decisions of district courts); 10 U.S.C. §§950c, 950f, 950g (2006) (includes de novo review of fact and law by CMCR followed by review as to matters of law, including sufficiency of the evidence, by the U.S. Court of Appeals for the District of Columbia Circuit). Note that the military commissions provide broader appeal rights and an additional level of appellate review than do civilian courts. See note 187, infra.


\textsuperscript{102} Hamdi v. Rumsfeld, 542 U.S. 520 (2004).

\textsuperscript{103} Hamdi, 542 U.S. at 520 ("Prisoners of war shall be released and repatriated without delay after the cessation of active hostilities") (quoting Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 118, Aug. 12, 1949, 6 U.S.T. 3316, 3406). With respect to some detainees, repatriation may pose challenges. See Kiyemba v. Obama, 605 F.3d 1046 (D.C. Cir. 2010) (per curiam).
is different from criminal prosecution, the legal process that applies is also different from that applicable in a criminal proceeding. In concluding that the detainees held at Guantánamo have a constitutional right to challenge the lawfulness of their detention by writ of habeas corpus, the Supreme Court in its Boumediene decision recognized that standards and procedures to be applied must account for the special circumstances of wartime detention, and left open the contours of the substantive and procedural law of detention for lower courts to shape in a common law fashion. Many of these detainee cases have been litigated recently in the federal courts in the District of Columbia, and some critical issues regarding the standards and procedures applicable to this unique class of cases have been resolved. For example, the courts have upheld the government’s standard as to who may be lawfully detained under the 2001 Authorization for Use of Military Force (AUMF), agreed that requiring the government to prove the lawfulness of detention by a preponderance of the evidence is constitutionally sufficient; and held that hearsay is admissible in these proceedings. Since Boumediene, the courts are in the process of implementing a regime that provides for rigorous review of the government’s evidence while properly accounting for the unique nature of the proceedings.

An exhaustive comparison of the differences among all three systems would require a longer discussion, but I have identified five relative

106. See Awad v. Obama, 608 F.3d 1, 10 (D.C. Cir. 2010).
107. See id. at 7.
108. Three additional caveats are in order. First, the extent and significance of the differences between the systems often turn on the facts of a particular case. There is no substitute for immersion in the details.

I am comparing civilian law enforcement and federal courts on the one hand, and use of our military detention authorities and military commissions on the other, but I want to emphasize that these are really three different tools, rather than two. For many of the reasons I mentioned, the two trial mechanisms – federal courts and military commissions – have more in common with each other than they do with law of war detention, which is not designed to hold individuals accountable for criminal conduct but instead to keep them away from the fight during a war. Both trial mechanisms also afford justice to the victims of terrorist attacks and significant community therapeutic value in a way that law of war detention cannot do. In federal criminal trials, the Crime Victims’ Rights Act, 18 U.S.C. §3771 (2006), provides victims of crimes with certain rights, including the right to reasonable, accurate and timely notice of public court proceedings related to the crime, §3771(a)(2), the right not to be excluded from public proceedings, §3771(a)(3), the right to confer with the government, §3771(a)(5), and the right to be heard by the court, §3771(a)(4), among others. Similarly, regulations issued by the Department of Defense in 2007 to govern the day-to-day functions of military commissions include the Military Commissions Victim and Witness Assistance Program (VWAP), which sets forth certain policies and responsibilities designed for the benefit of victims. See Regulation for Trial By
advantages of our military system and five of our civilian system, viewed solely from the perspective of the government and solely as to the effectiveness of each system in combating terrorism.\textsuperscript{109} Of course, in any particular case, all three of these systems – criminal justice, military, and law of war detention – may be lawful and appropriate, and determining which one to employ requires an assessment of the substantive and procedural features of each. I need to emphasize, however, that this comparison is not nearly as detailed a comparison as would be required in order to make informed policy or operational judgments. Those judgments generally would require comparisons that are far more granular and nuanced.

A. Advantages of Military Authorities

With those important caveats, here are five general advantages that using military authorities rather than civilian prosecution may offer to the government, depending on the facts:

1. Government's Burden

In federal court, prosecutors must persuade all twelve jurors beyond a reasonable doubt that the defendant is guilty of a federal offense.\textsuperscript{110} In

\textbf{MILITARY COMMISSIONS (RMC) (April 27, 2007 ed.),} available at http://www.defense.gov/news/Apr2007/Reg_for_Trial_by_MCM.pdf (RMC). These include, for example, that each crime victim should be notified of commission proceedings, see RMC 16-4b(2), be provided information about the conviction, sentencing, imprisonment, and transfer of the offender, RMC 16-4b(4), and be allowed to provide information, in writing, to any authority considering the offender's potential release or transfer from custody, RMC 16-4b(5). While these regulations implement the Military Commissions Act of 2006, Pub. L. No. 109-366 (2006), these provisions should not be affected by the Military Commissions Act of 2009, Pub. L. No. 111-84 (2009).

Third, I want to acknowledge that while I have experience with civilian criminal procedure, I am not an expert on military justice or the law of war. I have tried to describe accurately the rules governing law of war detention and military commissions, and I have tried also to be detailed, rigorous, and objective in the comparisons I draw. But there is a lot of complexity here, the military commission system is evolving, and I welcome any insight and nuance from those with greater expertise or a different perspective. My primary goal here is to start a conversation about the relative advantages and disadvantages of military authorities and civilian law enforcement, not to finish that conversation.

109. I do not mean to suggest that the perspective of the prosecution is the only viable perspective in assessing "advantages" of one system or another. As explained in Parts I and II, supra, that perspective is critical to those who would exclude the use of law enforcement from U.S. counterterrorism options, and hence a focus of this discussion. Nor do I mean to suggest that there are only five advantages and disadvantages of each system.

110. Andres v. United States, 333 U.S. 740, 748 (1948) ("Unanimity in jury verdicts is required where the Sixth and Seventh Amendments apply. In criminal cases this requirement of unanimity extends to all issues – character or degree of the crime, guilt and punishment – which are left to the jury."); FED. R. CRIM. P. 31(a) (unanimous jury
military commissions, the burden of proof is the same, but in non-capital cases only two-thirds of the members of the commission — in effect, the jurors — need to be persuaded for a guilty verdict, and the minimum number of jurors required is only five.\textsuperscript{111} The potential for non-unanimous guilty verdicts, as well as working with a smaller number of jurors, is a significant advantage to the government in a military commission, although there are important nuances that qualify that advantage in certain cases.\textsuperscript{112} For law of war detention where habeas corpus applies, the burden is different and often less demanding, which is to be expected given the different underlying basis for detention of enemy forces in war. Although the detainee has a right to an adversary proceeding before a federal judge,\textsuperscript{113} as noted above, requirement); Coffin v. United States, 156 U.S. 432, 453 (1895) (presumption of innocence); In re Winship, 397 U.S. 338, 364 (1970) (due process requires prosecution to prove defendant guilty of each element beyond a reasonable doubt).\textsuperscript{111} See 10 U.S.C. §949(c) (requiring members be instructed that accused is presumed innocent until guilt is established beyond a reasonable doubt); 10 U.S.C. §949m(a) (requiring two-thirds of members present to convict). Sentences of ten years or less also require concurrence of two-thirds of the members present at the time the vote is taken. 10 U.S.C. §949m(b)(1). Sentences above ten years, including life imprisonment, require the concurrence of three-fourths of the members present at the time the vote is taken. 10 U.S.C. §949m(b)(3). And imposition of capital punishment, which is discussed in greater detail, infra Part IV.B.4, requires a unanimous vote. 10 U.S.C. §949m(b)(2)(D). Because in non-capital cases, a minimum of only five members is required on the commission, 10 U.S.C. §948m(a), only three members may actually be needed to find guilt in order to convict — which is less demanding than the concurrence of twelve jurors to convict required in federal court. (In capital cases before a military commission, a minimum of twelve members is generally required, unless "reasonably unavailable . . . because of physical conditions or military exigencies," but there must be at least nine. 10 U.S.C. §949m(c).\textsuperscript{112} If the vote of the members of a military commission results in any fewer than two-thirds in favor of conviction, the accused will be acquitted; the two-thirds requirement only applies to convictions in military commissions whereas the unanimity requirement in federal court applies to all verdicts. Thus, for example, where the jury votes 7-5 in favor of conviction, the result in a military commission is an acquittal (because 7/12 is less than 2/3), while the result in federal court is a mistrial and retrial (because the verdict is not unanimous). Compare 10 U.S.C. §949m(a) ("No person may be convicted by a military commission except . . . by concurrence of two-thirds of the members present at the time the vote is taken") with Fed. R. Crim. P. 31(a) ("The verdict must be unanimous.") and 31(b)(3) ("The government may retry any defendant on any count on which the jury could not agree."). For a discussion of the requirements in capital cases, see text and notes 171-175, infra.\textsuperscript{113} See Boumediene v. Bush, 553 U.S. 723, 770-777 (2008) ("We do consider it uncontroversial that the privilege of habeas corpus entitles the prisoner to a meaningful opportunity to demonstrate that he is being held pursuant to "the erroneous application or interpretation" of relevant law."); id. at 784 ("For the writ of habeas corpus, or its substitute to function as an effective and proper remedy in this context, the court that conducts the habeas proceeding must have the means to correct errors that occurred during the [prior] proceedings. This includes some authority to assess the sufficiency of the Government's evidence against the detainee. It must also have the authority to admit and consider relevant exculpatory evidence that was not introduced during the earlier proceeding.").
the government need only persuade the judge by a preponderance of the evidence that the petitioner is part of, or substantially supporting, al Qaeda, the Taliban, or associated forces.\footnote{See Al Bihani v. Obama, 590 F.3d 866, 872 (D.C. Cir. 2010) (authority to detain under 2001 AUMF, includes “those who are part of forces associated with al Qaeda or the Taliban or those who purposefully and materially support such forces in hostilities against U.S. Coalition partners.”); see also Barhoumi v. Obama, 609 F.3d 416, 424 (D.C. Cir. 2010) (setting out same standard for government proof but noting that court “has yet to delineate the precise contours of the ‘part of inquiry’”). This discussion does not address any independent Constitutional power that may exist with respect to detention.} This can be a significant advantage in many cases where the individual’s affiliation with the enemy is clear but proof of a specific criminal offense would be difficult. That said, this burden is by no means a blank check; indeed, the review has been rigorous and it has been difficult for the government to carry this burden in a number of cases.\footnote{As of December 20, 2010, district courts have granted writs of habeas corpus in 21 contested cases. Writs have been denied in 19 cases. In addition, writs were granted with respect to 17 Chinese Uighurs whose cases the government did not oppose. Of the seven resolutions on appeal to date, four denials of the writ have been upheld by the D.C. Circuit, one denial of the writ has been reversed and remanded, and two grants of the writ have been reversed and remanded. Eight government appeals and eleven detainee appeals are pending, as well as four petitions for certiorari. Approximately 150 cases are pending either in the district court or on appeal.}

2. Admissibility of Confessions

As a general matter, military commissions have different and more flexible standards than federal courts for admitting custodial statements of the accused — although the differences are not as stark as the public debate might suggest. As discussed above, if the government wants to use a defendant’s responses to custodial interrogation in federal court, it generally must provide Miranda warnings,\footnote{See Miranda v. Arizona, 384 U.S. 436 (1966); New York v. Quarles, 467 U.S. 649 (1984). Under the public safety exception, an un-Mirandized statement made by a suspect immediately after a bombing or attempted bombing — concerning, for example, what the explosives were made of, or whether he had any accomplices — would likely be admissible in a criminal case against him. In one case, following the discovery of pipe bombs and related material in a raid on the defendant’s apartment, officers asked the defendant a number of questions about the bombs without advising him of his rights, including whether he planned to kill himself in an explosion. The court upheld the admission of the defendant’s un-Mirandized responses based on the public safety exception. United States v. Khalil, 214 F.3d 111, 121-122 (2d Cir. 2000).} and it must show that the statements were voluntary based on the totality of the circumstances (Miranda warnings are one important factor that helps establish voluntariness).\footnote{Haynes v. Washington, 373 U.S. 503, 513-514 (1963); United States v. Morris, 247 F.3d 1080, 1090 (10th Cir. 2001) (confession voluntary despite 19-year-old’s 10th grade education because he was given and understood his Miranda rights). The fruits of an involuntary confession may also be excluded from evidence in a criminal trial, Nix v. Williams, 467 U.S. 431, 442. n.3 (1984), unless they would “inevitably have been validly obtained.”}
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL 41

Under the 2009 MCA, Miranda warnings are not required, but a voluntariness test applies," subject to an exception for statements taken incident to military operations at the point of capture or during closely related active combat engagement." While statements elicited by torture or cruel, inhuman, or degrading treatment (CID) are per se excluded," evidence derived from those statements or other involuntary statements is

discovered" even without the coercive conduct, id. at 446, or if discovered through a source independent of the coercive conduct, id. at 443, or if the causal connection between the coercive conduct and the acquisition of the evidence is sufficiently attenuated, Wong Sun v. United States, 371 U.S. 471, 488 (1963). Cf. United States v. Ghali, ___ F. Supp. 2d ___, 2010 WL 4058043 at *1 (S.D.N.Y. Oct. 6, 2010) (excluding witness testimony in federal criminal trial because government failed to show that testimony was sufficiently attenuated from coercive government conduct so as to be admissible). The fruits of a voluntary but un-

118. 10 U.S.C. §948r(c). See, e.g., Prosecuting Law of War Violations: Reforming the Military Commissions Act of 2006: Hearing Before the Senate Armed Servs. Comm., 111th Cong., (2009) (statement of Vice Admiral Bruce E. MacDonald, Judge Advocate General, U.S. Navy), available at http://democrats.armedservices.house.gov/index.cfm/20097/prosecuting-law-of-war-violations-reforming-the-military-commissions-act-of-2006 ("And I think, at this point, we would assess it this way: The closer you are to the battlefield, the more that voluntariness would recede and you would look at the kind of indicia of reliability of the statement itself. At some point, though, as you take the detainee off the battlefield, and as you put them in a confinement facility, then the nature of the interrogation changes. So you go from this tactical interrogation . . . on the battlefield in Afghanistan. You move away from the intelligence interrogations that go on. And at some point, you're starting to look at exploitation, getting statements for prosecution. At that point I think we all agree that voluntariness should be the standard at that point.").

119. 10 U.S.C. §948r(c) ("A statement of the accused may be admitted in evidence in a military commission under this chapter only if the military judge finds – (1) that the totality of circumstances renders the statement reliable and possessing sufficient probative value; and (2) that – (A) the statement was made incident to lawful conduct during military operations at the point of capture or during closely related active combat engagement, and the interests of justice would best be served by admission of the statement into evidence; or (B) the statement was voluntarily given."). In determining voluntariness, the statute directs the military judge to consider the "totality of the circumstances," including, as appropriate: (1) the details of taking the statement, accounting for the circumstances of the conduct of military and intelligence operations during hostilities; (2) characteristics of the accused, such as military training, age, and education level; and (3) the lapse of time, change of place, or change in identity of the interrogators between the statement sought to be admitted and any prior questioning. 10 U.S.C. §948r(d). Some of the relevant terms – such as "at the point of capture" or "closely related active combat engagement" – are not defined in the 2009 MCA and clarification of their scope will develop through judicial interpretation and application on a case-by-case basis. It is unclear, for example, the extent to which such an exception can apply off the "traditional" battlefield, particularly in the United States. The precise contours of the due process analysis that courts will apply with regard to voluntariness of statements in military commissions are also unclear, and it is possible that in certain circumstances courts might find that these narrow statutory carve-outs for voluntariness may not meet due process requirements.

120. 10 U.S.C. §948r(a).
not explicitly barred in the 2009 MCA.\textsuperscript{121} On the other hand, in a military
commission, the judge must also find a statement "reliable" before it can be
admitted (which is not specifically required in federal court) and military
judges applying a similar reliability standard in a court martial sometimes
require corroboration of statements in ways that federal judges may not.\textsuperscript{122}

In a habeas corpus proceeding over law of war detention, there is
likewise no Miranda requirement, and thus no statements are excluded
based on the absence of a Miranda warning or failure to provide counsel.
Judges typically evaluate a statement using standards that are similar to
those that inform a voluntariness assessment, but perhaps weighted
differently, and at times they also seem to assess the statement’s reliability.
Although the government does not rely on statements that were the product

\textsuperscript{121} While there is no explicit bar on the "fruits" of such impermissible statements in
the 2009 MCA, the 2010 Military Commissions Manual does contain certain restrictions on
the admissibility of the "fruits" of statements obtained through torture, and cruel, inhuman,
or degrading treatment and other excludable statements, although admissibility of such
evidence will nevertheless be broader in federal courts, particularly as to the
admissibility of evidence derived from statements that were not elicited by torture or CID
but may nevertheless be deemed involuntary. Rule 304(a)(5) provides, for example, that
evidence derived from statements obtained by torture or cruel, inhuman, or degrading
practice may not be received in evidence against the accused who made the statement, if
the accused makes a timely motion to suppress or an objection, "unless the military judge
meets or a preponderance of the evidence that . . . the evidence would have been
obtained even if the statement had not been made; or . . . the use of such evidence would
otherwise be consistent with the interests of justice." U.S. DEP'T OF DEF., MANUAL FOR MIL.
COMM’NS (2010), Rule 304(a)(5)(A). Evidence derived from other excludable statements of
the accused (e.g., statements excluded because they were involuntary and did not meet any
exceptions to the voluntariness requirement, but not obtained through torture or cruel,
inhuman, or degrading treatment) may not be admitted against the accused who made the
statement if the accused makes a timely objection "unless the military judge determines by a
preponderance of the evidence that . . . the totality of the circumstances renders the evidence
reliable and possessing sufficient probative value; and . . . use of such evidence would be
consistent with the interests of justice." \textit{Id}. Rule 304(a)(5)(B). It remains unclear how
judges will treat such evidence in practice, and the extent to which due process protections
will apply to exclude such evidence. See, e.g., United States v. Ghanani, 2010 WL 4058043
at *19 n.182 (noting that it is "very far from clear" that evidence found to be derived from
corroboration and excluded from a federal criminal trial would be admissible in military
committees under Rule 304 or the Fifth Amendment).

2007) ("To be admitted, an accused's confession must be corroboration by evidence
sufficient to justify an inference that the essential facts of the confession are true [citing
Military Rule of Evidence (Mil. R. Evid.) 304(g)]. Corroborating evidence need not
establish all of the elements of the offense, nor establish the truth of the confession by even a
preponderance of the evidence. Only a 'slight' or 'very slight' quantum of evidence is
needed to fulfill the corroboration requirement of Mil. R. Evid. 304(g).") (internal citations
omitted). It is unclear what factors will be relevant to a finding that the statement is
sufficiently "reliable" in the military commission context – in particular, whether any
corroboration will be needed. If military judges do require some corroboration, even if only
minimal, this could complicate the admissibility question, especially for statements made
years after the events in question.
of torture, issues concerning allegedly coerced statements have often been litigated. Judges have discounted or rejected statements where there was evidence of coercion or a coercive environment,\textsuperscript{123} but they have often evaluated similar evidence in different ways in determining when coercive circumstances will invalidate a confession. One judge, for example, has suggested that the fact that statements are made in a facility where abuse was taking place, regardless of whether the petitioner himself was subject to it, may be sufficient to taint the statement.\textsuperscript{124} Other judges have differed in the extent to which they have credited claims of coercion, requiring more specific allegations.\textsuperscript{125} The judges also appear to disagree as to when prior abuse will taint subsequent statements; some judges have admitted statements made well after credited allegations of abuse as long as they were made at administrative hearings, while others have excluded such statements.\textsuperscript{126} The law continues to develop on these issues on a case-by-

\textsuperscript{123} See Al Warafi v. Obama, 704 F. Supp. 2d 32, 40 (D.D.C. 2010) (not relying on certain statements because "[r]espondents have not provided any evidence demonstrating that these statements are accurate, reliable, and credible. In particular, respondents have not assured the Court that these statements were not coerced. In addition, respondents have determined that at least one of the detainees on whose statements they rely is unreliable."); Hatim v. Obama, 677 F. Supp. 2d 1, 12 (D.D.C. 2009) ("[P]etitioner Hatim's unrefuted allegations of torture undermine the reliability of the statements made subsequent to his detention at Kandahar."); Ahmed v. Obama, 613 F. Supp. 2d 51, 61 (D.D.C. 2009) ("The larger issue is that [unnamed witness'] initial identification suffers from serious reliability problems. First and foremost, the detainee made the incriminating statement at Bagram Prison in Afghanistan, about which there have been widespread, credible reports of torture and detainee abuse.").

\textsuperscript{124} See Ahmed, supra note 123, 613 F. Supp. 2d at 61.

\textsuperscript{125} See, e.g., Awaad v. Obama, 646 F. Supp. 2d 20, 24 n.2 (D.D.C. 2009) (dismissing petitioner's claim that incriminating statements he made were the result of coercion and thus unreliable, noting only one specific allegation of coercion and Government's response), aff'd, 608 F.3d 1 (D.C. Cir. 2010).

\textsuperscript{126} See, e.g., Salahi v. Obama, 710 F. Supp. 2d 1, 6 (D.D.C. April 9, 2010) ([A]buse and coercive interrogation methods do not throw a blanket over every statement, no matter when given, or to whom, or under what circumstances. Allegations of mistreatment certainly taint petitioner's statements, raising questions about their reliability . . . . But at some point -- after the passage of time and intervening events, and considering the circumstances -- the taint of abuse and coercion may be attenuated enough for a witness's statements to be considered reliable -- there must certainly be a 'clean break' between the mistreatment and any such statement.", vacated and remanded on other grounds, Salahi v. Obama, 625 F.3d 745, 747 (D.C. Cir. 2010). Compare Anam v. Obama, 696 F. Supp. 2d 1, 9 (D.D.C. 2010) (finding the majority of petitioner's past statements unreliable with exception of two made during Combatant Status Review Tribunal (CSRT) and Administrative Review Board (ARB) hearings because the circumstances were "fundamentally different" from those affecting previous interrogations, representing a "sufficient 'break' from past coercive conditions") with Hatim, 677 F. Supp. 2d at 10-12 (unrefuted allegations of torture undermine reliability of subsequent statements, including those made to CSRT).
case basis, and there will be greater clarity over time on the circumstances under which the courts will consider a detainee’s statements.

3. Closing the Courtroom

Closing the courtroom may be helpful in some terrorism proceedings to protect classified information from public disclosure. It may be somewhat easier to close the courtroom in a military commission than in a federal criminal prosecution, and it is clearly easier to do so in civil habeas corpus proceedings challenging law of war detention. Under the Constitution, a federal criminal trial is presumptively open, and may be closed only upon a specific finding by the trial judge “that closure is essential to preserve higher values and is narrowly tailored to serve that interest.”127 Consistent

127. Press-Enterprise Co. v. Superior Court, 464 U.S. 501, 510 (1984); Walter v. Georgia, 467 U.S. 39, 48 (1984) (finding closure of entire suppression hearing was unjustified, applying Press-Enterprise test); id. at 45 (“The Court has made clear that the right to an open trial may give way in certain cases to other rights or interests, such as the defendant’s right to a fair trial or the government’s interest in inhibiting disclosure of sensitive information. Such circumstances will be rare, however, and the balance of interests must be struck with special care.”); 28 C.F.R. §30.5; U.S. Atty’s Manual §9-5.150. At this point, it remains unclear the extent to which this same Constitutional standard would apply to military commission proceedings. If it were held to apply, the practice of closure in military commissions would likely be more comparable to the practice in federal courts—in which courtrooms can and have been closed during testimony in hearings and trial proceedings, but only on rare occasions, and typically to protect the identity and safety of witnesses. See, e.g., United States v. Marzook, 412 F. Supp. 2d 913, 925-927 (N.D. Ill. 2006) (applying Walter and Press-Enterprise and permitting closure of courtroom during CIA-governed testimony of foreign agents during suppression hearing); United States v. Marrero, 04 Cr. 48 (S.D.N.Y. 2007) (JSR) (oral order) (courtroom closed during trial testimony of undercover officer); see also United States v. Holy Land Foundation, 04 Cr. 240, Doc. # 628 (N.D. Tex. 2007) (unpublished opinion and order) (permitting foreign agents to testify under pseudonym and courtroom to be partially closed during testimony, with only defendants, counsel, and immediate families present in addition to court personnel and jury; video feed of live testimony provided to public with identities of witnesses protected; certain other measures adopted to protect classified information including presence of agents’ legal advisor during testimony to permit consultation as to whether answer to questions would elicit classified information and question-by-question review by court about any classification issues); United States v. Salah, 03 Cr. 978, Doc. #652 (N.D. Ill. 2006) (unpublished opinion and order) (permitting foreign agents to testify under pseudonym and courtroom to be partially closed during testimony, with only defendants, counsel, and immediate families present in addition to court personnel and jury; video feed of live testimony provided to public; and transcript available to public upon request); United States v. Leos-Hernosillo, 213 F.3d 644, 2000 WL 300567, at *1 (9th Cir. Mar. 22, 2000) (district court granted motion to exclude public from courtroom during trial testimony of a confidential informant, but provided simultaneous audio feed, which was affirmed by the 9th Circuit in a summary order); see also United States v. Doc, 63 F.3d 121, 128 (2d Cir. 1995) (aplying Walter and Press-Enterprise in reviewing defendant’s motion to close the courtroom for safety reasons and stating that “the same test applies whether a closure motion is made by the government over the defendant’s Sixth Amendment objection or made by the defendant over the First Amendment objection of the government or press”). Cf. Ayala v.
with this standard, courts have also implemented special procedures — such as the “silent witness rule” — in some cases to shield classified information from disclosure to the public attending a trial, which is similar in many respects to closing the proceeding as to the evidence in question. Under the 2009 MCA, a military judge may close all or part of a trial to the public in potentially broader circumstances, but must still make a determination that closure is necessary to protect information which, if disclosed, would be harmful to national security interests or to the physical safety of any participant. Moreover, in contrast to federal judges, military judges have more practical references for the conduct of closed proceedings, as it is not uncommon for courts-martial to include closed sessions to admit classified evidence, an experience that will likely influence the practice in military commissions. Since habeas corpus proceedings take place in federal

Speckard, 131 F.3d 62, 72 (2d. Cir. 1997) (applying Waller and Press-Enterprise and upholding limited closure of courtrooms during trial testimony of undercover officers in three state court criminal cases).

128. The “silent witness rule” — which has also been used rarely — involves the employment of techniques, such as the use of numbers or code names for a person or location, the key to which only the trial participants and the jury have access, or documents containing classified information which is only available to the witness, court, counsel, and jury. As a consequence, only they can understand trial testimony or evidence employing the coded terms or related to the document, and the testimony is not comprehensible to members of the public. See, e.g., United States v. Rosen, 520 F. Supp. 2d 786, 794, 798-799 (E.D. Va. 2007) (“silent witness” rule, by which “certain evidence designated by the government is made known to the judge, the jury, counsel, and witnesses, but is withheld from the public . . . results in closing a part of the trial to the public” and accordingly the practice is permitted, but only after applying Press-Enterprise criteria); see also United States v. Zeitl, 835 F. 2d 1059, 1063 (4th Cir. 1987) (noting use of procedure whereby classified document referred to by witness in testimony was available only to court, counsel, jury, and witness but declining to reach question of the propriety of this approach); United States v. Abu Ali, 538 F.3d 210, 255, n.22 (4th Cir. 2008) (noting silent witness rule procedure “contemplates situations in which the jury is provided classified information that is withheld from the public, but not from the defendant” but declining to rule expressly on whether it would be proper).

129. 10 U.S.C. §949d(c). Military commission trials also have implemented a 45-second delay of the broadcast of statements to permit classified information to be blocked before it is aired in certain cases; this ensures, for example, that if the accused were to say something out loud that is classified, it can be blocked before the audience hears it. As far as I know, federal courts have not thus far adopted such a mechanism, which could raise both practical and legal concerns.

130. In fact, training for military judges includes specific instructions regarding the conduct of closed sessions of trials in accordance with case law. Cf. United States v. Grunden, 2 M.J. 116, 120-121 (C.M.A. 1977) (finding exclusion of public from virtually entire espionage trial violated Sixth Amendment right to public trial of accused in court-martial; however, in order to protect classified or security matters “within carefully limited guidelines, partial exclusion of the public . . . can be justified”). Military courts also permit the sealing of transcripts of trial testimony in limited circumstances, which is not practiced to the same extent in federal court. Additionally, because the jurors are military officers, they have security clearances that civilians may not, making the disclosure of classified information less of a problem. However, even in military trials, defendants are not excluded

223
courtrooms, they are also theoretically open to the public. However, as a practical matter, the vast majority of district court habeas proceedings involving Guantánamo Bay detainees have been closed in order to protect classified information. Although in the large majority of cases counsel see the same classified material the court sees, the habeas petitioner has no right to review classified material or even to be present at the hearing. Arrangements are made for petitioners to listen from Guantánamo to unclassified opening statements, and they often testify in their cases via video link. The classified portions of the district court proceedings are closed, however, and involve only the judge, counsel and other court personnel. Appellate proceedings have required the filing of public briefs (in which classified material is redacted) and oral arguments have generally been open to the public, with the court holding additional closed sessions when necessary.

4. Admissibility of Hearsay

It is sometimes in the government's interest in a terrorism case to be able to introduce hearsay evidence - statements from an individual who is not present in the courtroom to testify and be cross-examined. For example, use of hearsay may be the only way (or the best way) to introduce evidence from a sensitive intelligence source. The Confrontation Clause of the Sixth Amendment presents barriers to the introduction of testimonial hearsay in federal criminal proceedings in a way that may not apply in the military commissions, though the application of different constitutional provisions to the military commissions is as yet unclear. The 2009 MCA permits hearsay in broader circumstances than in the federal court system. It expressly provides that hearsay evidence may be admitted if the military judge finds, among other things, that direct testimony from the witness is "not available as a practical matter, taking into consideration the physical location of the witness, the unique circumstances of military and intelligence operations during hostilities, and the adverse impacts on military or intelligence operations" that would likely result from requiring production of the witness. (Of course, broader hearsay rules can also benefit the accused in a military commission prosecution.) The standard for admission of hearsay is even more relaxed in habeas proceedings even if trial testimony warrants closure of the courtroom to the general public.

131. See Crawford v. Washington, 541 U.S. 36, 53-54 (2004) ("[T]he Framers would not have allowed admission of testimonial statements of a witness who did not appear at trial unless he was unavailable to testify, and the defendant had a prior opportunity for cross-examination.").


134. In fact, in Hamdan's military commission trial, Hamdan himself relied far more than the government on the more flexible military commission rule.
brought to challenge law of war detention, where hearsay is permissible and the hearsay evidence is assessed for reliability.\textsuperscript{135} Even though hearsay evidence is admissible in such proceedings, the courts have assessed hearsay evidence based on its indicia of reliability and whether it is consistent with the evidence as a whole. Assessment of the weight given hearsay evidence can be very fact-dependent.\textsuperscript{136}

5. Classified Evidence

In federal courts, the use of classified evidence is governed by the Classified Information Procedures Act (CIPA)\textsuperscript{137} and interpretive case law. CIPA permits the government to provide the defense a substitute for classified information, such as a statement admitting the relevant facts or a summary, if the court finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information itself.\textsuperscript{138} The new rules in the 2009 MCA on handling classified information are modeled on CIPA.

\textsuperscript{135} See Al Bihani v. Obama, 590 F.3d 866, 879 (D.C. Cir. 2010) (hearsay "is always admissible" in habeas proceedings); see also Odah v. United States, 611 F.3d 8, 14 (D.C. Cir. 2010) (district court's reliance on hearsay "is of no consequence. To show error in the court's reliance on hearsay evidence, the habeas petitioner must establish not that it is hearsay, but that it is unreliable hearsay."). (quoting Awad v. Obama, 608 F.3d 1, 5). As a general matter, evidentiary and procedural rules in habeas proceedings are less rigid, and are at the discretion of individual judges. See Boumediene v. Bush, 553 U.S. 723, 795 (2008) ("We make no attempt to anticipate all of the evidentiary and access-to-counsel issues that will arise during the course of the detainees' habeas corpus proceedings. We recognize, however, that the Government has a legitimate interest in protecting sources and methods of intelligence gathering; and we expect that the District Court will use its discretion to accommodate this interest to the greatest extent possible."). These and the other remaining questions are within the expertise and competence of the District Court to address in the first instance.") (internal citation and quotation omitted). See also In re: Guantanamo Bay Detainee Litigation, Misc. No. 08-0442 (TFH), Case Management Order, 05-cv-00634-RWR, Doc. # 85 (D.D.C. Nov. 6, 2008) at n.1 (noting individual judges can depart from general framework set forth in case management order (Guantanamo Litigation CMO); Order on Government's Motion for Clarification, 05-cv-02444-RMC, Doc. #52 (D.D.C. Dec. 16, 2008) (Guantanamo Litigation Amended CMO).

\textsuperscript{136} Appellate decisions have set out a framework for district courts to use in approaching evidence in these habeas proceedings. See, e.g., Adahi v. Obama, 613 F. 3d 1102, 1105-1110 (D.C. Cir. 2010) (providing framework for assessing evidence as a whole); Al Odah v. United States, 609 F.3d at 427-432 (similar to Adahi, in viewing evidence as a whole); Barbouni v. Obama, 609 F.3d 416, 427-432 (examining reliability of diary based on its characteristics and details); Awad, 608 F.3d at 7-10 (upholding detention after carefully reviewing multiple different types of hearsay and discussing reliability); Benisah v. Obama, 610 F.3d 718, 725-727 (D.C. Cir. 2010) (reversing and remanding where key document was not adequately corroborated but providing that multiple pieces of evidence, each independently unreliable, can be mutually corroborative).

\textsuperscript{137} 18 U.S.C. App. 3.

\textsuperscript{138} 18 U.S.C. App. 3 §6(c).
and are not dramatically different, but do have some modifications or improvements based on experience in terrorism cases in federal court. While the fundamental procedures are now very similar, the 2009 MCA makes explicit some rules that have been developed in federal court only through judicial interpretation and practice. The 2009 MCA also clarifies other provisions that have sometimes resulted in more restrictive federal court precedent, and provides additional avenues to protect intelligence.

139. For example, the 2009 MCA makes clear that courts can conduct an ex parte pre-trial conference with either party to address potential classified information issues; CIPA's language is silent on this issue but has been interpreted to allow such conferences. Compare 10 U.S.C. §949p-2(b) (court shall hold conference to consider classified information “ex parte to the extent necessary to protect classified information from disclosure, in accordance with the practice of the Federal courts under” CIPA), with 18 U.S.C. App. 3 §2 (no discussion of whether pre-trial conference can be ex parte or not, and United States v. Campa, 529 F.3d 980, 994-995 (11th Cir. 2008) (permitting ex parte conference); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) (permitting ex parte conference). In addition, classified procedures in the 2009 MCA clearly apply not only to documentary material but also to testimony, which again is not clear from the language of CIPA. Compare 10 U.S.C. §949p-4(b) (“The military judge . . . may authorize the United States - (A) to delete or withhold specific items of classified information; (B) to substitute a summary for classified information; or (C) to substitute a statement admitting the relevant facts that the classified information or material would tend to prove.”), with 18 U.S.C. App. 3 §4 (“The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents . . . to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.”). The CIPA provision has nevertheless been judicially applied by analogy to non-documentary material. See United States v. Moussaoui, 333 F.3d 509, 513-515 (4th Cir. 2003) (while concluding that CIPA did not specifically cover testimony, lower court applied procedures set forth in CIPA by analogy for deposition of witnesses). Also, the 2009 MCA mandates, rather than simply permits, the judge to consider the government’s motion for relief ex parte. Compare 10 U.S.C. §949p-4(b)(2) (“military judge shall permit” ex parte presentation in lieu of declaration from government setting forth alleged damage to national security that discovery of or access to specified information may cause), with 18 U.S.C. App. 3 §4 (“court may permit the United States to make a request . . . to be inspected by the court alone”), and United States v. Rezaq, 156 F.R.D. 514, 526 (D.D.C. 1995) (precluding government from filing CIPA §4 pleading ex parte), reconsidered at 899 F. Supp. 697, 707 (government must litigate its right to proceed ex parte in an adversarial hearing) with Klimavicius-Viloria, 144 F.3d at 1261 (upholding use of ex parte submissions). For an additional comparison of the 2009 MCA and CIPA, see Response 28 in Oversight of the U.S. Dept. of Justice: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (2009) (Responses to questions for the record by Atty Gen. Eric Holder (Mar. 22, 2010).

140. For example, 10 U.S.C. §949p-3 expressly provides the court the ability to design measures or to issue an order to protect against the disclosure of classified information produced in discovery or “that has otherwise been provided to, or obtained by” the accused; in contrast, CIPA’s language permits such protective orders for classified information “disclosed by the United States to any defendant in any criminal case in any district court of the United States,” 18 U.S.C. App. 3 §3. The CIPA provision has been interpreted by one federal court as not authorizing courts to issue protective orders prohibiting the defendant from publicly disclosing, outside of court proceedings, information he may have obtained prior to the criminal case. See United States v. Pappas, 94 F.3d 795, 800-801 (2nd Cir. 1996) (under CIPA “information acquired by the defendant prior to the criminal prosecution may
sources, methods, and activities. As a result, litigation risks for the
government on classified information issues may be somewhat reduced in
military commissions as compared to federal courts. That said, CIPA has
generally worked well in protecting classified information in federal courts,
which have much more experience handling classified information issues
than the military commissions. The 2009 MCA specifically requires
military judges to view federal court precedent as authoritative unless the
text of the 2009 MCA specifically requires a different result.

The rules regarding disclosure of classified evidence in habeas cases
are both more flexible and less certain than in either civilian criminal courts
or in military commissions. Generally the individual judges have greater
discretion to set procedures and, as noted above, there is more flexibility to
shield classified information from the detainee himself and, in exceptional
cases, even from the detainee’s counsel. However, the government is often
required to provide declassified versions of documents to the detainees and
their counsel. Because the evidence submitted in habeas cases typically
includes hundreds of pages of intelligence reports, the declassification
process poses serious logistical challenges to the government and risks the

be prohibited from disclosure only ‘in connection with the trial’ and not outside the trial”).
The 2009 MCA language clarifies that this is too restrictive a reading of the provision’s
scope.

Another example of where the 2009 MCA clarifies provisions of CIPA that have been
restrictively applied by courts is with regard to the scope of interlocutory appeals. Compare
10 U.S.C. §950d(c) (permitting interlocutory appeal by United States “whenever the military
judge enters an order or ruling that would require the disclosure of classified information,
without regard to whether the order or ruling appealed from was entered under this chapter,
another provision of law, a rule, or otherwise.”), with 18 U.S.C. App. 3 §7(a) (permitting
interlocutory appeal by United States “from a decision or order of district court authorizing
the disclosure of classified information, imposing sanctions . . . , or refusing a protective
order sought by the United States to prevent the disclosure of classified information.”). The
CIPA provision has been interpreted, for example, to preclude interlocutory appeal of an
order authorizing a defendant in a criminal case to depose a witness who may have
possessed classified information on the basis that, because the deposition order did not
involve the discovery of classified documentary information under CIPA, 18 U.S.C. App. 3
§4, it was not an order “authorizing the disclosure of classified information” under CIPA and
therefore not subject to interlocutory appeal. See Mousaoui, 333 F.3d at 280 (Wilkins, C.J.,
concurring); see also Oversight of the U.S. Dept’t of Justice: Hearing Before the S. Comm.
http://judiciary.senate.gov/hearings/testimony.cfm?id=4470&wit_id= (“The military
commissions, the modifications that have been made to the secrecy provisions, really codify,
I think, what judges do as a matter of routine in civilian court — with one exception, and that
has to do with the possibility of interlocutory appeals, which, frankly, I think is a good idea
and perhaps ought to be incorporated into what we do on the civilian side. Much of the
other enhancements that you see with regard to military commissions reflect what judges do
on the civilian side.”).

141. 10 U.S.C. §949p-6(c)(2) (protection of sources, methods, and activities by which
evidence is acquired).
142. 10 U.S.C. §949p-1(d).
inadvertent release of information that should remain classified. Nonetheless, on the whole, habeas proceedings, where it is common to close the courtroom and which permit hearsay evidence, provide the government the greatest ability to protect classified information, although there are challenges associated with reliance on classified hearsay evidence.\textsuperscript{143}

B. Advantages of Civilian Authorities

Subject to the same caveats as described above, here are five general advantages (for the prosecution) of using federal courts rather than military commissions or law of war detention:

1. Certainty and Finality

The civilian criminal justice system enjoys an advantage over both military commissions and law of war detention with respect to the certainty of its rules and the finality of its results. The federal courts have years of experience trying and convicting dangerous criminals, including international terrorists, and the rules are well-established and understood. To be sure, there is substantial litigation in many federal terrorism prosecutions, and some of the more complex cases may present novel legal issues. But while military commissions have long roots in American history during times of armed conflict, the current commissions are essentially a new creation, and they do not have the body of established procedures and years of precedent and experience to guide the parties and the judges. This invites, if it does not guarantee, challenges to virtually every aspect of the commission proceedings – the legality of the system, the jurisdiction of the court, the lawfulness of certain offenses, the rules on the use of evidence derived from coerced statements, discovery obligations, and the nature of protective orders (among others). Indeed, legal challenges to the new commissions authorized by the 2009 MCA were initiated in the fall of 2009 and early 2010.\textsuperscript{144} While most of these challenges have recently

\textsuperscript{143}. It is important to note the interrelationship between hearsay rules and classified evidence. As explained above, military commissions have relatively rigorous hearsay admissibility rules as compared to habeas proceedings; however, there is greater scope for admitting hearsay in military commissions than in federal criminal trials. This broader scope for hearsay evidence in military commissions relative to federal criminal trials, combined with the CIPA-based provisions in the 2009 MCA, can provide the government with some additional ways to use and protect classified information in certain military commission cases, particularly to protect sources and methods, that may not be available in federal criminal cases.

\textsuperscript{144}. For example in 2009, detainees filed mandamus petitions in the D.C. Circuit requesting that the military commissions be halted. They alleged, among other claims, that the commissions exceeded Congressional authority and impermissibly discriminated against aliens. See Bin Al Shihb Petition, supra note 99, at 2-3, 35; Al Hawsawi Petition, supra note.
been dismissed as moot, the underlying substantive issues have not been resolved yet, meaning that we may not have confidence in military commission convictions until each case works its way up to the Supreme Court – a process that could take years.

Similarly, habeas challenges to law of war detention for Guantánamo Bay detainees have raised claims about every aspect of that process, including the rules for the proceedings and even the basic scope of the government’s detention authority. While trial judges have varied in their understanding of who can be detained and what evidentiary procedures and sources of law apply, some of the most significant substantive and procedural questions have recently been resolved by the court of appeals. Nevertheless, it will likely take a substantial period of time before the appellate review of Guantánamo cases has developed the degree of uniformity or predictability that we have after many years of trying terrorism and other criminal cases in federal court. Whether law of war detention is even legally available for individuals who are apprehended in

99, at 3; In re Abdal-Rahim Nashiri, No. 09-1274 (D.C. Cir. Nov. 20, 2009) (raising issue of alienage/citizenship distinction) (hereinafter Nashiri Petition); In re Mohammed Kamin, No. 09-1294 (D.C. Cir. Nov. 30, 2009) (same), dismissed as moot, July 22, 2010 (hereinafter Kamin Petition). Since the military commissions had been suspended at the time these petitions were filed, the D.C. Circuit held them in abeyance. See Orders of D.C. Circuit Court of Appeals, In re Hawsawi, No. 09-1244 (Dec. 12, 2009); In re Bin Al Shibh, No. 09-1239 (Dec. 16, 2009); In re Nashiri, No. 09-1274 (Jan. 5, 2010); In re Kamin, No. 09-1294 (Jan. 22, 2010). On July 23, 2010, no military proceedings having been initiated by then, the D.C. Circuit issued orders dismissing three of the petitions on mootness grounds. See Orders of D.C. Circuit Court of Appeals, In re Hawsawi, No. 09-1244 (July 23, 2010); In re Bin Al Shibh, No. 09-1239 (July 23, 2010); In re Kamin, No. 09-1294 (July 23, 2010). As of October 20, 2010, the Nashiri Petition was still pending. In March 2010, a petition was filed by Omar Khadr that was also later dismissed by the D.C. Circuit, raising some of the same claims as well as an additional one. See In re Mohammed Khadr, No. 10-1067 (Mar. 23, 2010) (raising challenges to military commissions based on alienage distinction; claim that issuance of evidentiary rules violates the Ex Post Facto clause; and claim that defendant’s status as “child soldier” forecloses prosecution by military commission). dismissed, August 4, 2010 (hereinafter Khadr Petition). Khadr pleaded guilty to the charges against him in October 2010. See News Release, U.S. Dept’t of Defense, Detainee Pleads Guilty at Military Commission Hearing (October 25, 2010), available at http://www.defense.gov/releases/release.asp?releaseid=13999. The one detainee who has been convicted after a military commission trial and remains in detention has filed an appeal, challenging the conviction on the grounds that, Inter alia, none of the crimes of conviction – conspiracy and providing material support to terrorism – constitute war crimes properly triable by a military commission. See Brief of Appellant at 2, 24, United States v. Ali Hamza Ahmad Suliman al Balhul, CMCR Case No. 09-001 (Sept. 1, 2009). In addition, a second detainee, who was convicted upon a plea of guilty and is no longer in custody, has also filed an appeal that raises a similar challenge to his material support conviction, among other issues. See Brief of Appellant, at 3, 22, United States v. Salim Ahmed Handan, CMCR Case No. 09-002 (Oct. 15, 2009). As of February 2011, these appeals remain pending.
the United States is another major area of uncertainty (and controversy), as litigation on that issue has yielded diverse opinions from our courts.\footnote{An en banc panel of the Fourth Circuit, reversing a prior panel opinion, held 5-4 that the President has the authority to detain as an enemy combatant a lawful resident alien initially apprehended in the United States by civilian authorities and subsequently transferred to military custody. See Al-Marri v. Pucciarelli, 534 F.3d 213, 253-262 (4th Cir. 2008) (TrAXLER, J., concurring), judgment vacated and appeal dismissed as moot; Al-Marri v. Spagnone, 129 S. Ct. 1545 (2009) (mem.). The judges took widely varying views of the question, resulting in eight different opinions. In contrast, the Second Circuit held that the President did not have the authority to detain as an enemy combatant an American citizen seized on American soil outside a zone of combat. Padilla v. Rumsfeld, 352 F.3d 695, 698 (2d Cir. 2003), reversed on other grounds, Rumsfeld v. Padilla, 542 U.S. 426 (2004). For a more detailed discussion of this issue, see infra note 147.}

was a guilty plea.147 Thereafter, in 2009, Congress overhauled the rules governing commissions (for the second time) in the 2009 MCA, and two more detainees have since pleaded guilty under the new system.148

147. The three convictions prior to enactment of the 2009 MCA are as follows:

On February 2, 2007, David Hicks was charged with one count of providing material support for terrorism and one count of attempted murder in violation of the law of war. See Memorandum for Detainee David M. Hicks, Re: Notification of the Swearing of Charges (Feb. 2, 2007), available at http://www.defense.gov/news/d2007hicks%20-%20notification%20so%20sworn%20charges.pdf. On March 30, 2007, he pleaded guilty to the charge of providing material support to terrorism. See News Release, U.S. Dep’t of Defense, Detainee Convicted of Terrorism Charge at Guantanamo Trial (Mar. 30, 2007), available at http://www.defense.gov/releases/release.aspx?releaseid=10678. As part of a pre-trial agreement, Hicks’s sentence was limited to not more than nine months’ confinement; a military commission panel sentenced him to seven years of confinement of which six years and three months were suspended per the pre-trial agreement. Id. Pursuant to a transfer agreement, Hicks was transferred to Australia to serve the remainder of his sentence after his conviction. Id.


148. As noted above, legal challenges to the newly-authorized commissions began in 2009; while most have been dismissed on procedural grounds the substantive issues have not
Commissions should in the end prove to be a powerful tool in the current war, but for now the uncertainty is a factor to be weighed. In that sense, military commissions are like a new weapons system – one that is based on venerable principles and has been in development for nearly a decade, but has been test-fired only a handful of times (and has had to be redesigned twice). The civilian criminal justice system, by contrast, has been used many times against terrorists both before and after 9/11, and untold hundreds of thousands of times in other cases. With two such weapons available – one new and promising but relatively untested, and the other proven and reliable even if subject to some limits – who would send troops into battle armed only with the first?  


On October 25, 2010, Khadr pleaded guilty to the charges against him, which included murder in violation of the law of war, attempted murder in violation of the law of war, conspiracy, providing material support for terrorism, and spying. See News Release, U.S. Dep’t of Defense, Detainee Pleads Guilty at Military Commission Hearing (Oct. 25, 2010), available at http://www.defense.gov/releases/release.aspx?releaseid=13999. He was sentenced to 40 years’ imprisonment by a military jury on October 31, 2010. Under the terms of his plea agreement, he will serve eight years (in addition to time served), and, pursuant to a diplomatic agreement with Canada, one year will be in U.S. custody followed by his return to Canada to serve the remainder of his sentence. See News Release, U.S. Dep’t of Defense, DOD Announces Sentence for Detainee Omar Khadr (Oct. 31, 2010), available at http://www.defense.gov/releases/release.aspx?releaseid=14023.

149. I emphasize that I do not mean by this analogy to suggest that military commissions do not work, that they are not or will not be effective, or that they should be used only in a secondary role behind the criminal justice system. I mean only to say that we should recognize the challenges inherent in implementing a new system; we should be able
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL 55

2. Scope

The criminal justice system is a tool with broader application in many instances than either military commissions or law of war detention. The criminal justice system can be used against any person who has violated our criminal laws, whether here or abroad, if our laws apply extraterritorially, as many of them do. In contrast, the government interprets the 2001 AUMF as informed by law-of-war principles, as authorizing detention of those who are part of, or who substantially support, Taliban, al Qaeda, or associated forces that are engaged in hostilities against the United States or its coalition partners. Individuals who are part of or supporting other

to overcome those challenges in time, but we should not deny their existence now.

150. Such extraterritorial offenses include (but are not limited to) war crimes (including grave breaches of the 1949 Geneva Conventions, violations of certain provisions of the Hague Rules, and grave breaches of Common Article 3), 18 U.S.C. §2441; extraterritorial assault or murder of a U.S. national or conspiracy to do so for reasons related to terrorism, 18 U.S.C. §2332; use of a weapon of mass destruction against, inter alia, a U.S. national outside the United States, 18 U.S.C. §2332a; acts of terrorism transcending national boundaries, 18 U.S.C. §2332b; bombings of places of public use including offenses against another state or government facility, 18 U.S.C. §2332f; the deployment of missiles or missile systems to destroy aircraft, 18 U.S.C. §2332g; harboring or concealing terrorists, 18 U.S.C. §2339; providing material support to terrorists, 18 U.S.C. §2339A; providing material support to foreign terrorist organizations, 18 U.S.C. §2339B; providing financing to terrorism, 18 U.S.C. §2339C; receiving military training from a foreign terrorist organization, 18 U.S.C. §2339D; torture when the offender is present in the United States, 18 U.S.C. §2340A; offenses against a U.S. national (including murder, rape, assault, etc., on the premises of an overseas U.S. diplomatic, consular, military or other U.S. government mission or a residence related thereto), 18 U.S.C. §7(9); destruction of aircraft (including certain foreign aircraft), 18 U.S.C. §32; violence at international airports, 18 U.S.C. §37; assaults against U.S. government personnel in the performance of their official duties, 18 U.S.C. §111; assaults against internationally-protected persons (including such conduct overseas when the offender is afterwards found in the United States), 18 U.S.C. §112; knowing development, possession, etc., of a biological agent, 18 U.S.C. §175; knowing development, possession, etc., of a chemical weapon (including extraterritorial deployment against a U.S. person of facility), 18 U.S.C. §229; receipt, use, possession, etc., of nuclear materials, 18 U.S.C. §831; use of fire or explosive, inter alia, to destroy U.S. government property, or to commit any other federal offense, 18 U.S.C. §844(f); conspiracy to kill, maim or injure persons or damage property in a foreign country, 18 U.S.C. §956; travel to a foreign country for the purpose of taking part in a military enterprise against a friendly nation, 18 U.S.C. §960; using or carrying a firearm during in relation to the commission of a federal crime of violence, or possession of a firearm to facilitate such an offense, 18 U.S.C. §924(e); killing or attempting to kill officers or employees of the United States on account of or in the performance of official duties, 18 U.S.C. §1114; murder or manslaughter of internationally protected persons, 18 U.S.C. §1116; hostage taking (extraterritorial jurisdiction if the victim is a U.S. national or if the hostage taker is "found in the United States"), 18 U.S.C. §1203; treason, 18 U.S.C. §2381; seditious conspiracy, 18 U.S.C. §2384; and aircraft piracy, 49 U.S.C. §46502.

151. This discussion does not address any independent constitutional detention authority that may exist.

152. The court of appeals has upheld that standard. See Al Bhani v. Obama, 590 F.3d
terrorist groups like Hamas, Hizbollah, or the FARC are not subject to the AUMF based solely on that membership; nor are lone-wolf terrorists who may be inspired by al Qaeda but are not part of it. There is also a question whether law of war detention extends to persons apprehended in the United States. The application of military commissions is in some ways even

866, 872 (D.C. Cir. 2010) ("We have no occasion here to explore the outer bounds of what constitutes sufficient support or indicia of membership to meet the detention standard. We merely recognize that both prongs are valid criteria that are independently sufficient to satisfy the standard."). The court rejected the proposition that the international laws of war inform the scope of the AUMF, but in denying rehearing en banc, seven judges of the court determined that the panel’s statements regarding international law were unnecessary to the decision. See Al Bihani v. Obama, 619 F.3d 1, 1 (D.C. Cir. 2010).

153. See, e.g., Hamdli v. Obama, 616 F. Supp.2d 63, 75, n. 17 (D.D.C. 2009) (agreeing with government that AUMF provides “authority to detain members of ‘associated forces’ as long as those forces would be considered co-belligerents under the law of war” but “‘falsified forces’ do not include terrorist organizations who merely share an abstract philosophy or even a common purpose with al Qaeda – there must be an actual association in the current conflict with al Qaeda or the Taliban”).

154. See Bensayah v. Obama, 610 F.3d 718, 725 (D.C. Cir. 2010) ("It is impossible to provide an exhaustive list of criteria for determining whether an individual is ‘part of’ al Qaeda. That determination must be made on a case-by-case basis by using a functional rather than a formal approach and by focusing upon the actions of the individual in relation to the organization. That an individual operates within al Qaeda’s formal command structure is surely sufficient but is not necessary to show he is ‘part of’ the organization; there may be other indicia that a particular individual is sufficiently involved with the organization to be deemed part of it . . . . but the purely independent conduct of a freelancer is not enough.") (internal quotations and citations omitted); Hamdli, 616 F. Supp. 2d at 75 ("[M]ere sympathy for or association with an enemy organization does not render an individual a member’ of that enemy organization. The key inquiry, then, is not necessarily whether one self-identifies as a member of the organization (although this could be relevant in some cases), but whether the individual functions or participates within or under the command structure of the organization – i.e., whether he receives and executes orders or directions.") (quoting Gherebi v. Obama, 609 F. Supp. 2d 43, 69 (D.D.C. 2009)).

155. The statutory and constitutional questions raised by detention in the United States have divided our courts. Two (and only two) persons apprehended in this country in recent times have been held under the law of war. First, Jose Padilla was arrested on a federal material witness warrant on May 8, 2002, and was transferred to law of war custody approximately one month later, on June 9, 2002, after his court-appointed counsel moved to vacate the warrant. He was returned to the civilian criminal system in January 2006, and convicted in August 2007 after a three-month trial. He was sentenced to 17 years and 4 months’ imprisonment in January 2008. Ali Saleh Kahlah Al-Marri was initially approached by the FBI and interviewed in October and December 2001. He was arrested on December 12, 2001 on a material witness warrant, and he was indicted on federal criminal charges (non-terrorism related) on February 6, 2002 in the Southern District of New York. After those charges were dismissed for lack of venue, he was re-indicted on similar charges in the District of Illinois on May 22, 2003. On June 23, 2003 he was transferred to military detention. He was permitted access to counsel in October 2004. In February 2009, he was indicted again in Illinois. He pleaded guilty in April 2009 to providing material support to al Qaeda and was sentenced to 8 years in prison in October 2009.

In both of these cases, the transfer to law of war custody raised serious legal issues in the courts concerning the lawfulness of the government’s actions and spawned lengthy litigation. In Padilla’s case, the United States Court of Appeals for the Second Circuit found
that the President did not have the authority to detain him under the law of war. Padilla v. Rumsfeld, 352 F.3d 695, 723-724 (2d Cir. 2003) (finding that the detention was not authorized either by statute: "[t]he plain language of the [AUMF] contains nothing authorizing the detention of American citizens captured on United States soil, much less the express authorization . . . and the ‘clear,’ ‘unmistakable’ language required . . ."; or the Constitution: "in the domestic context, the president’s inherent constitutional powers do not extend to the detention as an enemy combatant of an American citizen seized within the country away from a zone of combat"; and thus ordering that the Secretary of Defense release Padilla from military custody within 30 days and the government transfer him to "appropriate civilian authorities who can bring criminal charges against him") (internal citations omitted). The Supreme Court ultimately reversed and remanded that decision on the grounds that Padilla’s habeas petition had been filed in the wrong jurisdiction. Rumsfeld v. Padilla, 542 U.S. 426, 451 (2004). Padilla then re-filed his habeas petition in the District of South Carolina, the district where he was being held. The district court granted habeas relief, based on reasoning similar to that of the Second Circuit, and ordered that he be criminally charged or released. Padilla v. Hanft, 369 F. Supp. 2d 678, 689, 692 n. 14 (D.S.C. 2005), reversed, Padilla v. Hanft, 423 F.3d 386 (4th Cir. 2005). A panel of the Fourth Circuit reversed, concluding that the AUMF conferred the requisite detention authority on the President, 423 F.3d at 389. While the petition for certiorari seeking review of the Fourth Circuit decision was pending before the Supreme Court, the government indicted Padilla, and the petition was accordingly denied by a divided Supreme Court. Hanft v. Padilla, 547 U.S. 1062 (2006). Three Justices would have granted certiorari. id.

In Al-Marri’s case, a divided panel of the United States Court of Appeals for the Fourth Circuit initially held that Al-Marri’s detention was unlawful, rejecting the Government’s argument that the AUMF provided authority for military detention of enemy combatants in the United States, and that the President had inherent Constitutional authority to order Al-Marri’s detention. Al-Marri v. Wright, 487 F.3d 160, 184 (4th Cir. 2007) ("Thus the Government is mistaken in its representation that Hamdi and Padilla ‘recognized’ [the President’s authority to detain ‘enemy combatants’ during the current conflict with al Qaeda]. No precedent recognizes any such authority. Hamdi and Padilla evidence no sympathy for the view that the AUMF permits indefinite military detention beyond the ‘limited category’ of people covered by the ‘narrow circumstances’ of these cases.") (internal citations omitted); id. at 193 ("We do not question the President’s war-time authority over enemy combatants; but absent suspension of the writ of habeas corpus or declaration of martial law, the Constitution simply does not provide the President the power to exercise military authority over civilians within the United States."). On rehearing en banc, this decision was reversed on a 5-4 split vote, resulting in eight separate opinions, and the majority of judges found that Al-Marri had not been afforded adequate due process to challenge his detention as an enemy combatant. Al Marri v. Pucciarelli, 554 F.3d 213, 253-262 (4th Cir. 2008) (Traxler, J., concurring). No single opinion in Al Marri commanded a majority of the court. The Supreme Court vacated this decision as moot after Al-Marri was indicted and transferred back to the criminal justice system. Al Marri v. Spagone, 129 S. Ct. 1545 (2009) (mem.).

Notably, because the authority to detain individuals for purposes of trial by military commission is similarly rooted in the law of war, Hamdan v. Rumsfeld, 548 U.S. 557, 596-597 (2006) (noting that “law-of-war commission” is the only model for military commission used outside the contexts of enemy-occupied territory or martial law); (“Not only is its jurisdiction limited to offenses cognizable during time of war, but its role is primarily a fact-finding one — to determine, typically on the battlefield itself, whether the defendant has violated the law of war.”) (Stevens, J., plurality opinion), any military commission prosecution of aliens apprehended in the United States might also be challenged on the ground that detention authority is lacking.
narrower: Not only must a defendant be an unprivileged enemy belligerent with the requisite connection to al Qaeda or the Taliban, he must also be a foreign national. U.S. citizens like José Padilla, John Walker Lindh, and Anwar Awlaki cannot be prosecuted by military commission, even if they are part of al Qaeda or associated forces.156

In our criminal justice system, Congress has enacted a vast array of federal laws that criminalize most types of terrorist conduct, including terrorist acts abroad against U.S. nationals, material support to terrorism or a designated terrorist organization, harboring terrorists, terrorist financing, receiving military training from a terrorist organization, narco-terrorism, hostage taking, aircraft piracy, sea piracy, bombings of public places, WMD-related offenses, and many others, as well as conspiracies to commit these crimes. (To the extent that these statutes were recently enacted or amended, they may not be available to charge older crimes,197 and criminal charges under Title 18 require some jurisdictional nexus to the United States or its interests, often specified in the elements of certain extraterritorial crimes.)198 In addition to pure terrorism-related offenses, as I have explained,199 prosecution of ordinary crimes can also neutralize terrorists—just as Al Capone was convicted of tax fraud rather than murder. In contrast, a military commission has limited jurisdiction only to prosecute violations of the laws of war and offenses traditionally triable by military commissions.200

156. 10 U.S.C. §948c ("Any alien unprivileged enemy belligerent is subject to trial by military commission as set forth in this chapter."); 10 U.S.C. §948a(1) ("The term 'alien' means an individual who is not a citizen of the United States."). An unprivileged enemy belligerent is an individual who has engaged in or purposefully and materially supported hostilities against the United States or its coalition partners, or was a part of al Qaeda at the time of the alleged offense. 10 U.S.C. §§948a(7) & (8).

157. For example, 18 U.S.C. §2339A, which prohibits the provision of material support to terrorism, was originally confined to offenses occurring within the United States. The requirement of territoriality was eliminated by the PATRIOT Act in 2001. Accordingly, extraterritorial offenses are subject to prosecution under this provision only if their commission (or a portion thereof) post-dates October 2001. Likewise, 18 U.S.C. §2339B, which prohibits providing material support to foreign terrorist organizations (FTOs), was amended in 2004 to generally reach extraterritorial offenses. See IRTPA §2001(c)(1). Its utility in reaching material support offenses involving FTOs is therefore similarly limited to offenses that post-date the 2004 amendment.

158. See, e.g., 18 U.S.C. §2332a (use of weapons of mass destruction) (criminalizing offenses either against a national of the United States or within the United States, §2332a(a), or by a national of the United States outside the United States, §2332a(b)).

159. See supra Part III.A.

160. See 10 U.S.C. §948d (military commissions shall have jurisdiction over any offense set forth in the 2009 MCA or in articles 104 and 106 of the Uniform Code of Military Justice (UCMJ), or made punishable by the law of war). There are 32 enumerated offenses in the 2009 MCA. See 10 U.S.C. §950b. Moreover, several key offenses included in the 2009 MCA, such as conspiracy and material support to terrorism, 10 U.S.C. §§950d (25) & (29), will likely be challenged by defense counsel on the ground that they have no analog in the common law of war and cannot constitutionally be applied to conduct that
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL 59

With respect to law of war detention, of course, no criminal charges need be established at all. It must be proved, however, that the individual is part of al Qaeda, the Taliban, or associated forces. In some cases, it can actually be harder to make this showing than to prove a criminal offense. For example, where someone in the United States travels to Afghanistan or Pakistan to obtain terrorist training in a camp, we may be able to prove the federal offense of receiving military training from a terrorist organization, but unless the training camp is linked to al Qaeda, the Taliban, or an associated force, we may be unable to prove that the individual is detainable under the AUMF. Likewise, we may be able to prove that an individual was involved in a specific act of terrorism—such as the federal offenses of conspiring to kill persons in a foreign country, or providing assistance in the development of chemical weapons—but face similar obstacles to proving that he is subject to detention under the AUMF.

predated Congress’ enactment of the offenses in statute. For example, four justices of the Supreme Court have expressed some doubt about the viability of the conspiracy offense in a military commission, albeit before Congress expressly authorized this offense in law. Hamdan, 548 U.S. at 603-612 (Stevens, J., plurality opinion). It is unclear what impact Congressional authorization will have on this question. Cf. id. at 601 (noting that “[t]here is no suggestion that Congress has, in exercise of its Constitutional authority . . . positively identified ‘conspiracy’ as a war crime.”). Both Bahlul and Hamdan raised these issues in appeals of their military commission convictions, which are currently pending. See supra note 144. While we hope and expect to defeat any legal challenges to military commission charges, the outcome of such litigation is uncertain.

161. 18 U.S.C. §2339D. To establish a violation of this statute, the government must prove: (1) the defendant knowingly received military-type training; (2) the training was received from or on behalf of a designated foreign terrorist organization; (3) the defendant had knowledge at the time of the offense that the organization was a designated foreign terrorist organization or that the organization engaged in terrorism or terrorist activity; and (4) the existence of one of the following jurisdictional requirements: the defendant is a national of the United States, an alien with lawful permanent resident status, or a stateless person whose habitual residence is the United States; the prohibited conduct occurred in whole or in part within the United States; after the conduct the defendant was brought to or found in the United States; the offense occurred in or affected interstate or foreign commerce; or the defendant aided and abetted conduct which satisfied these elements. See, e.g., Transcript of Guilty Plea, United States v. Bryant Neal Vinas, 68 Cr. 823, Doc. #23 (NGG) (E.D.N.Y. Jan. 28, 2009).

162. 18 U.S.C. §956(a)(1). The government must prove: (1) the defendant agreed with at least one person to commit murder; (2) the defendant willfully joined the agreement with the intent to further its purpose; (3) during the existence of the conspiracy, one of the conspirators committed at least one overt act in furtherance of the conspiracy; and (4) at least one of the conspirators was within the jurisdiction of the United States when the agreement was made. See United States v. Wharton, 320 F.3d 526, 537-538 (5th Cir. 2003).

163. 18 U.S.C. §229(a). The government must prove: (1) the defendant assisted or induced others to develop, produce, acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, use, or threaten to use, a chemical weapon; (2) the defendant provided this assistance or inducement knowingly; and (3) the existence of one of the following jurisdictional requirements: the prohibited conduct took place in the United States, took place outside of the United States and was committed by a national of the United States, was
3. Incentives for Cooperation

The criminal justice system has mechanisms to encourage cooperation by detainees that do not exist in law of war detention or are not as well-established or extensive in military commissions. As I have explained, the criminal justice system has long-standing experience with proffer agreements, plea agreements, pre-sentencing incentives available under the U.S. Sentencing Guidelines, and post-sentencing incentives available under the Federal Rules of Criminal Procedure. These tools can be used to encourage cooperation and obtain intelligence. The government's promises to the defendant are judicially enforceable, and the defendant's failure to follow through on his promises can be sanctioned, which increases the likelihood that cooperation agreements will be made and honored. In the military commission system, Rule 705 provides a mechanism similar to a plea agreement which is based on an analogous procedure used in the courts-martial system. Through it, the parties may negotiate a pre-trial agreement, including an agreement to cooperate and an applicable sentencing range. However, this system and its effectiveness in obtaining committed against a citizen of the United States while the citizen was outside the United States, or was committed against any property that was owned, leased, or used by the United States or any department or agency of the United States, whether the property is within or outside the United States. See Charge Given in United States v. Kassir, S2 04 Cr. 356 (JGK) (S.D.N.Y.).

164. See supra Part III.A.

165. U.S.S.G. §5K1.1; FED. R. CRIM. P. 35.

166. See Brady v. United States, 397 U.S. 742, 755 (1970) ("A plea of guilt entered by one fully aware of the direct consequences, including the actual value of any commitments made to him by the court, prosecutor, or his own counsel, must stand unless induced by threats (or promises to discontinue improper harassment), misrepresentation (including unfulfilled or unfulfillable promises), or perhaps by promises that are by their nature improper as having no proper relation to the prosecutor's business (e.g., bribes") (internal quotation and citation omitted).

167. See MANUAL FOR COURTS-MARTIAL, UNITED STATES 705 (2008), available at http://www.jag.navy.mil/documents/mcm2008.pdf. There is also a practice in courts-martial whereby the accused can provide information and be granted limited immunity, akin to a plea agreement. This may also be available in military commissions, although the practice is not as established as it is in federal criminal cases.

168. See U.S. DEP'T OF DEF., MANUAL FOR MILITARY COMMISSIONS 705 (2010). The rule provides that the accused and the convening authority may enter in a pretrial agreement consistent with the rule. The agreement must be in writing and contain all of the terms of the agreement. Id. 705(a). The agreement may include, inter alia, a promise by the accused to plead guilty to or stipulate to certain charges; and a promise by the convening authority to refer charges to a certain type of military commission; refer a capital offense as noncapital; or withdraw one or more of the charges or specifications; have trial counsel present no evidence of one or more of the specifications; take specified action on the sentence adjudged by the commission; and fulfill any additional terms or conditions requested by the accused that are within the convening authority's power and not otherwise barred by the Manual or the MCA. Id. 705(b). In order for a term or condition to be enforceable, the accused must freely and voluntarily agree to it; and no agreement is enforceable if it deprives the accused...
cooperation in a military commission case — where the equivalent of the jury does the sentencing, the cases can take years to resolve, and there has been no significant experience with cooperation to date — is not yet well tested. Moreover, there are no sentencing guidelines, no mandatory minimums, and no track record that can be used to set the parameters for any negotiations, which may make it more difficult to come to an agreement. Nor is there an extensive practice of post-conviction, pre-sentencing cooperation, particularly for a substantial period of time (as may be required in complex terrorism cases), or an established post-sentencing cooperation mechanism in military commissions. The federal courts, in contrast, have all of these tools readily available for use.

In law of war detention, although interrogators can offer detainees improvements in their conditions of confinement (e.g., better recreational opportunities) in return for cooperation, there are currently no established and enforceable mechanisms for encouraging cooperation analogous to those available in the criminal justice system. There is no “sentence” over which to negotiate, nor is there any neutral third party like a judge who could enforce any agreement to release an individual at a date certain in return for cooperation. Detainees may have little incentive to provide information when that information may be used against them only to prolong their detention, with no end in sight. On the other hand, in law of war detention, if the individual is held in an area where habeas corpus does not apply and the detainee has no right to counsel, interrogators can control the conditions of detention and interrogation in lawful ways, including separating the detainee from others, that many believe can be helpful to the effective interrogation of a hardened terrorist in particular cases. In some cases, this may be an effective approach to intelligence collection. However, this approach may not be as effective, at least not for any extended period of time (which may be necessary to yield results), in any area where habeas corpus and right to counsel applies.

In sum, in law of war detention, the absence of enforceable mechanisms for balancing conditions and duration of confinement against cooperation of the right to counsel or to “other indispensable judicial guarantees.” Id. 705(c)(1). Permissible conditions include a promise to enter into a stipulation of fact; a promise to testify as a witness in the trial of another; and a promise to waive certain procedural rights, including appellate review, among others. Id. 705(c)(2). No member of the military commission shall be informed of the existence of the agreement. Id. 705(c).

169. See, e.g., U.S. DEP’T OF ARMY, FIELD MANUAL FM 2-22.3, HUMAN INTELLIGENCE COLLECTOR OPERATIONS, APPENDIX M (RESTRICTED INTERROGATION TECHNIQUE — SEPARATION) ¶¶M-1, M-5 (Sept. 2006) (“The purpose of separation is to deny the detainee the opportunity to communicate with other detainees in order to keep him from learning counter-resistance techniques or gathering new information to support a cover story; [and] decreasing the detainee’s resistance to interrogation. . . Separation will be applied on a case-by-case basis when there is a good basis to believe that the detainee is likely to possess important intelligence and [other] intelligence approach techniques. . . are insufficient.”).
may in some cases reduce the incentive for cooperation-based intelligence collection. Similarly, in military commissions, the absence of specific mechanisms to facilitate cooperation that are as well-established or extensive as in federal courts, contributes to making bargaining more unpredictable, and thus potentially less effective, in that forum. Plea bargaining is essentially a market transaction, and markets work best where there are clear, enforceable rules of contract and associated traditions. These rules and traditions do not spring up overnight; as in all systems, they take time to develop. Moreover, they develop best when the alternatives are clear, such as when the government’s authority to detain for a long, fixed period is unquestioned. A terrorist detained in the criminal justice system knows that the system itself is impregnable, and if the government has a strong case he will go to prison for a long time. A terrorist detained under the law of war, particularly if he is initially apprehended in the United States, faces an entirely different situation, in which the validity of the system is subject to challenge, the extent of his rights and the government’s power is less certain, and the duration of his confinement is indefinite. Likewise, in the military commission system, in addition to prevailing uncertainty about the system as a whole, the practical operation and usefulness of specific cooperation mechanisms imported from the courts-martial system remains unclear. The incentives created by uncertainty in both of the military systems may not lead to quick and effective cooperation.

4. Sentencing

Sentencing is more predictable, and potentially better for the government, in federal court than in a military commission. In the criminal justice system, as I mentioned, federal courts have for many years meted out lengthy prison sentences in the most serious terrorism cases, including a number of life sentences. While not every case results in a long sentence, and indeed many small fishes receive much shorter terms, sentencing is more or less predictable. Federal judges impose sentences based in part on the U.S. Sentencing Guidelines, which include provisions such as a

170. See Puckett v. United States, 129 S. Ct. 1423, 1430 (2009) (analyzing plea agreement as contract) ("When a defendant agrees to a plea bargain, the Government takes on certain obligations. If those obligations are not met, the defendant is entitled to seek a remedy, which might in some cases be rescission of the agreement, allowing him to take back the consideration he has furnished, i.e., to withdraw his plea. But rescission is not the only possible remedy; in [Sanabell v. New York, 404 U.S. 257, 263 (1971)] we allowed for a resentencing at which the Government would fully comply with the agreement—in effect, specific performance of the contract. . . . It is precisely because the plea was knowing and voluntary (and hence valid) that the Government is obligated to uphold its side of the bargain.") (internal citations omitted) (emphasis in original).

171. See supra notes 145, 155.
terrorism enhancement for certain offenders. In some cases, statutory minimum sentences apply, and maximum sentences may be up to life, and include death, for certain offenses. In the military commissions, by contrast, the sentence is imposed by the military members – essentially the jury – rather than the judge, and without the benefit of any guidelines or minimums enacted by Congress. While we have little experience so far with sentencing by the juries in the military commissions, as noted above, two of the five commission defendants sentenced thus far (including Osama bin Laden’s driver) received sentences of five to six years, with credit for time served at Guantánamo. They were therefore released within a few months. A third defendant received a life sentence that is now on appeal.

172. U.S. SENTENCING GUIDELINES §3A1.4 (terrorism enhancement) (“If the offense is a felony that involved, or was intended to promote, a federal crime of terrorism,” the offense level should be increased by 12 levels (and be no lower than level 32) and defendant’s criminal history category should be Category VI. The Guidelines are advisory, not mandatory. United States v. Booker, 543 U.S. 220 (2005). However, they provide a starting point and a framework for guidance on the appropriate sentence in a given case. See United States v. Gall, 552 U.S. 38, 49-50 (2007) (“[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark. The Guidelines are not the only consideration, however. Accordingly, after giving both parties an opportunity to argue for whatever sentence they deem appropriate, the district judge should then consider all of the [statutorily prescribed sentencing] factors to determine whether they support the sentence requested by a party. In so doing, he may not presume that the Guidelines range is reasonable. He must make an individualized assessment based on the facts presented. If he decides that an outside-Guidelines sentence is warranted, he must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance. We find it uncontroversial that a major departure should be supported by a more significant justification than a minor one.”) (citations omitted). Between October 1, 2008 and September 30, 2009, the most recent period for which annual statistics are available, approximately 37% of cases nationally were sentenced within the given Guidelines range. See U.S. SENTENCING COMM’N, SOURCEBOOK OF FED. SENTENCING STATISTICS (2009), Table N – National Comparison of Sentence Imposed and Position Relative to the Guideline Range: Fiscal Year 2009, available at http://www.ussc.gov/ANNUAL/2009/TableN.pdf. Of the remainder, approximately 2% were above the Guideline range; 25% were “Government Sponsored Below Range” (that is, either through a §5K1.1 motion, or other government supported sentencing reduction); and 16% were “Non-Government Sponsored Below Range.” Id.

173. Sentences of ten years or less require concurrence of two-thirds of the members present at the time the vote is taken. 10 U.S.C. §949m(b)(1). Sentences above ten years, including life imprisonment, require the concurrence of three-fourths of the members present at the time the vote is taken. 10 U.S.C. §949m(b)(3). The only statutory limits are a prohibition on cruel or unusual punishments, 10 U.S.C. §949a, and a requirement that the punishment “not exceed such limits” as are imposed by the President or Secretary of Defense for a particular offense. 10 U.S.C. §949i. Capital punishment is discussed in text and notes 182 and 183, infra.

More recently, a fourth was sentenced to two years and a fifth to eight years, both pursuant to guilty pleas. 175 Sentencing in the commissions is much harder to predict at this stage.

With respect to law of war detention, there is of course no “sentence” since it is not a criminal punishment at all, and the legally permissible duration of confinement is not clear. Under traditional principles, terrorists may be held under the authority afforded by the 2001 AUMF and the law of war until the end of hostilities. However, the Supreme Court has warned that if the circumstances of the current conflict “are entirely unlike those of the conflicts that informed the development of the law of war,” that authority to detain “may unravel.” 176 In the Hamdi decision, which upheld the detention of a U.S. citizen apprehended on the battlefield in Afghanistan, a plurality of the Court expressly relied on the fact that “active combat operations against Taliban fighters apparently are ongoing in Afghanistan” in concluding that the 2001 AUMF continued to authorize detention of enemy belligerents. 177 As circumstances change, or if active combat operations are concluded, it is not clear how long the detention authority will endure. 178 Right now, of course, with combat operations ongoing in Afghanistan and elsewhere, our authority to detain under the law of war remains solid.

175. See discussion about the guilty pleas and sentences of Ibrahim Al Qosi and Omar Khadr, supra note 148.
177. Id.
178. Id. In Hamdi, for example, a plurality of the Court acknowledged Hamdi’s concern that if the Court accepted the government’s view of its detention authority, he could potentially be detained for the rest of his life given the nature of the conflict. Although not directly resolving whether the AUMF authorized such indefinite detention, the Court narrowly described the detention authority it was upholding:

It is a clearly established principle of the law of war that detention may last no longer than active hostilities. . . . Hamdi contends that the AUMF does not authorize indefinite or perpetual detention. Certainly, we agree that indefinite detention for the purpose of interrogation is not authorized. Further, we understand Congress’ grant of authority for the use of ‘necessary and appropriate force’ to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel. But that is not the situation we face as of this date. . . . The United States may detain, for the duration of these hostilities, individuals legitimately determined to be Taliban combatants who ‘engaged in an armed conflict against the United States.’ If the record establishes that United States troops are still involved in active combat in Afghanistan, those detentions are part of the exercise of ‘necessary and appropriate force,’ and therefore authorized by the AUMF. Id. at 520-521 (citations omitted). In other contexts, the Supreme Court has indicated that the question of when an armed conflict ends is properly a question for the political branches, rather than the judiciary, to determine. See Ludecke v. Williams, 335 U.S. 160, 168-169 (1948).
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL 65

There are also significant advantages in how capital cases are handled in federal court as compared to a military commission. The federal criminal system has well-established procedures for how the government decides to seek the death penalty, and there is an experienced defense bar capable of handling the complex litigation required during the sentencing phase of the trial. The death penalty is imposed by a unanimous jury of twelve, and can be imposed after a trial or after a guilty plea. In military commissions, there is greater uncertainty about death penalty procedures than in the federal criminal system, as there is no recent experience in the commissions on this issue. While a capital sentence must be imposed unanimously, the number of military commission "jurors" who must vote need not be limited to twelve. Rather, the required number is however many have not been struck during the voir dire process — in other words, if twenty-one jurors are called for the panel, and none are struck, all twenty-one must vote for the death penalty for it to be imposed, making it potentially much harder for the prosecution to obtain the death penalty. Also, it is not clear at present that the death penalty can be imposed by a military commission after a guilty plea, and questions also remain about


180. As of January 2011, there were defendants who had been sentenced to the death penalty in the federal system. The last federal execution was in 2003; there have been three federal executions since the federal death penalty was reinstated in 1988. See Death Penalty Info. Ct., Federal Death Penalty, available at http://www.deathpenaltyinfo.org/federal-death-row-prisoners#list; Death Penalty Info. Ct., Federal Executions, 1927-2003, available at http://www.deathpenaltyinfo.org/federal-executions-1927-2003. In the court-martial system, as of September 2010, there were seven individuals sentenced to the death penalty. See Death Penalty Info. Ct., The U.S. Military Death Penalty, available at http://www.deathpenaltyinfo.org/us-military-death-penalty. The last military execution was in 1961. Id.

181. 10 U.S.C. §949m(b)(2)(D). In such a case, 14 votes (two-thirds of 21) would be needed to convict, while the full 21 would be needed to impose the death sentence.

182. 10 U.S.C. §949m(b)(1)(C) provides that the death penalty cannot be imposed in a military commission unless the "accused was convicted of the offense by the concurrence of all the members present at the time the vote is taken." When an accused pleads guilty, no vote is taken for conviction. Therefore, there is a question about whether the death penalty can be imposed after a guilty plea consistent with this provision. Based on the same language in the 2006 MCA, a military judge raised the issue and ordered briefing in December 2008; the question was not resolved before military commission proceedings were suspended by President Obama in January 2009. See Government Response to Military Judge's Directed Brief (Capital Punishment Issues), United States v. Khaled Sheikh Mohammed, No. MJ-010 (Dec. 22, 2008). The 2010 Military Commissions Manual contains the following on this issue, in non-binding commentary accompanying the rule governing guilty pleas: "In the discussion under this rule in the 2007 Manual for Military Commissions, the following sentence appeared: 'The M.C.A. permits an accused to plead guilty to a capital offense referred to a capital military commission, at which trial death remains an authorized sentence, notwithstanding the accused's plea of guilty.' That sentence has been omitted in the 2010 Manual. The omission of that sentence, however, does not suggest that an accused cannot accept responsibility for guilt in a capital case. In the event an accused desires to accept responsibility and avoid a lengthy proceeding on the question of
the availability of sufficiently trained defense counsel and adequate resources — all of which could further complicate post-conviction litigation.\(^{13}\) Of course, for detainees held in law of war detention without trial, capital punishment is not available at all.

5. International Cooperation

Finally, the criminal justice system may help us obtain important cooperation from other countries. That cooperation may be necessary if we want to detain suspected terrorists or otherwise accomplish our national security objectives. Our federal courts are well-respected internationally. There are well-established, formal legal mechanisms that allow the transfer of terrorism suspects to the United States for trial in federal court, and for the provision of information to assist in law enforcement investigations — i.e., extradition and mutual legal assistance treaties (MLATs). Our allies around the world are comfortable with these mechanisms, as well as with more informal procedures that are often used to provide assistance to the United States in law enforcement matters, whether relating to terrorism or other types of cases. Such cooperation can be critical to the success of a prosecution, and in some cases can be the only way in which we will gain custody of a suspected terrorist who has broken our laws.\(^{14}\)

In contrast, many of our key allies around the world are not willing to cooperate with or support our efforts to hold suspected terrorists in law of war detention or to prosecute them in military commissions. While we
hope that over time they will grow more supportive of these legal
mechanisms, at present many countries would not extradite individuals to
the United States for military commission proceedings or law of war
detention. Indeed, some of our extradition treaties explicitly forbid
extradition to the United States where the person will be tried in a forum
other than a criminal court. For example, our treaties with Germany
(Article 13)185 and with Sweden (Article V(3))186 expressly forbid extradition
when the defendant will be tried in an "extraordinary" court, and the
understanding of the Indian government pursuant to its treaty with the
United States is that extradition is available only for proceedings under the
ordinary criminal laws of the requesting state.187 More generally, the
doctrine of dual criminality — under which extradition is available only for
offenses made criminal in both countries — and the relatively common
exclusion of extradition for military offenses not also punishable in civilian
court may also limit extradition outside the criminal justice system.188 Apart
from extradition, even where we already have the terrorist in custody, many
countries will not provide testimony, other information, or assistance in
support of law of war detention or a military prosecution, either as a matter
of national public policy or under other provisions of some of our
MLATs.189

185. Treaty Between the United States of America and the Federal Republic of
186. Convention on Extradition Between the United States of America and Sweden,
187. See Exchange of Letters Between Strobe Talbott, Acting Secretary of State, United
States of America, and Saeed S. Shervani, Minister of State for External Affairs, India, of
June 25, 1997, attached to Extradition Treaty Between the Government of the United States
12873 (confirming understanding of both countries that "as a general matter, upon
extradition, a person shall be proceeded against or punished under the ordinary criminal laws
of the Requesting State, and shall be subject to prosecution or punishment in accordance
with the Requesting State's ordinary rules of criminal procedure. If either party is
considering prosecution or punishment upon extradition under other laws or other rules of
criminal procedure, the Requesting State shall request consultations and shall make such a
request only upon the agreement of the Requested State.").
188. Under the "dual criminality" doctrine, "an offense is extraditable only if the acts
charged are criminal by the laws of both countries." Collins v. Loisel, 259 U.S. 309, 311
(1922); United States v. Saccomo, 58 F.3d 754, 766 (1st Cir. 1995) (dual criminality
does not require laws be "carbon copies of one another" or have identical elements, rather it "is
deemed to be satisfied when the two countries' laws are substantially analogous.").
189. The Agreement on Mutual Legal Assistance between the United States and the
European Union, for example, includes a provision that "[a] request may be denied if it
relates to a military offense that would not be an offense under the ordinary criminal law."
See Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal
Assistance Between the United States of America and the European Union, U.S.-E.U., June
25, 2003, S. TREATY DOC. NO. 109-13 (2006). This provision has been incorporated into
the United States' treaties with individual member nations. See, e.g., id. (as to the
These concerns are not hypothetical. During the last Administration, the United States was obliged to give assurances against the use of military commissions in order to obtain extradition of several terrorism suspects to the United States. There are a number of terror suspects currently in foreign custody who likely would not be extradited to the United States by foreign nations if they faced military tribunals. In some of these cases, it might be necessary for the foreign nation to release these suspects if they


190. The following are two examples of cases in which the United States provided assurances that individuals would not be tried in military commissions in order to obtain their extradition to the United States:

- **Oussama Kassir**: In 2007, the Czech Republic extradited Kassir to the United States based on assurances that he would not be prosecuted in military tribunals. In 2009, Kassir was found guilty in federal court of providing material support to al Qaeda in connection with his participation in a plot to establish a jihad training camp in Oregon and was sentenced to life in prison.

- **Syed Hashmi**: In 2007, the United Kingdom extradited Hashmi to the United States based on assurances that he would not be prosecuted in military tribunals. He pleaded guilty in April 2010 to conspiring to provide material support to al Qaeda.

191. The following are some examples of cases in which the United States has had to provide assurances that individuals would not be tried in military commissions in support of pending extradition requests:

- **Mahmoud Said Omar**: Sought for trial in the District of Minnesota in connection with an ongoing investigation into the recruitment of young men in Minneapolis to train with or fight for al Shabaab in Somalia. Omar is pending extradition from the Netherlands.

- **Khalid Al Fawwaz and Adel Mohammed Almagid Abdul Bary**: Sought for trial in the Southern District of New York in connection with the bombing of the U.S. embassies in East Africa in 1998. They are pending extradition from the United Kingdom.

- **Nizar Trabelsi**: Sought for trial in the District of Columbia in connection with plotting with other al Qaeda operatives to commit terrorist attacks against U.S. targets in Europe. He is pending extradition from Belgium.

- **Babar Ahmad**: Sought for trial in the District of Connecticut in connection with providing material support for terrorists and money laundering; he also allegedly possessed a document accurately describing plans of a U.S. naval battle group operating in the Straits of Hormuz in April 2001. Ahmad is pending extradition from the United Kingdom.

- **Haroon Rashid Aswat**: Sought for trial in the Southern District of New York in connection with a plot to create a jihad training camp in the United States. Aswat is pending extradition from the United Kingdom.
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

cannot be extradited because they do not face charges pending in the
foreign nation.

On the other hand, in certain circumstances, some foreign partners have
indicated they are only willing to provide assistance in court proceedings if
their involvement can be kept secret. As noted above, the various fora have
different rules and procedures regarding protection of classified information
and closure of proceedings. None are foolproof and, in the individual case,
it may not be possible to protect such information regardless of the
proceeding, depending on its nature and importance. However, as a general
rule, habeas proceedings will provide the most flexibility to protect
information from public disclosure and, in particular cases, military
commissions may provide more such protections, through the interplay of
less restrictive hearsay rules and the classified information procedures, than
are available in federal courts.

The comparison set forth above is somewhat artificial, and it omits
several areas of difference, including differences in the right to counsel. 192

192. In the criminal justice system, once the Department of Justice commences
prosecution by presenting a terrorism suspect to a judge or indicting him, the suspect has a
right to the assistance of counsel, including during any interrogation (concerning the offense
for which he is charged). See Rothbery v. Gillespie County, 354 U.S. 191, 198 (2008)
(citations omitted); McNeil v. Wisconsin, 501 U.S. 171, 175 (1991); Texas v. Cobb, 532
U.S. 162, 168 (2001); Maine v. Moulton, 474 U.S. 159, 177, 180 n. 16 (1985). Similarly,
one individual is charged in a military commission, the MCA requires that military
counsel be provided to the defendant “as soon as practicable.” 10 U.S.C. §948k(a)(3).
In practice, this would be no later than when charges are referred, but the accused may be
provided counsel at the point that charges are sworn (if not before). In addition, even before
charges have been brought within the military commission system (or if they are never
brought), there are serious questions about the government’s authority to deny a suspected
terrorist inside the United States access to a lawyer to challenge his detention under the law
of war. As noted above (supra note 62) then-Judge Michael Mukasey ruled that Jose Padilla
was entitled to a lawyer to pursue a habeas petition when he was held in law of war
detention but not charged in a military commission. See Padilla v. Bush 233 F. Supp.2d 564,
605 (S.D.N.Y. 2002). In addition, the Supreme Court in 2004 indicated that Yasser Hamdi,
a U.S. citizen captured in Afghanistan, should have access to counsel to challenge his
detention, a point the government conceded in that case. Hamdi v. Rumsfeld, 542 U.S. 537,
559 (2004) (“Hamdi asks us to hold that the Fourth Circuit also erred by denying him
immediate access to counsel upon his detention and by disposing of the case without
permitting him to meet with an attorney. Since our grant of certiorari in this case, Hamdi
has been appointed counsel, with whom he has met for consultation purposes on several
occasions, and with whom he is now being granted unmonitored meetings. He
unquestionably has the right to access to counsel in connection with the proceedings on
remand.”). Of course, if detainees are held overseas under the law of war in an area where
habeas corpus does not apply, affording them access to counsel may not be required. In any
event, as discussed above (see supra text and notes 58-59, 62), involvement of counsel, or
advising a detainee of his right to counsel, does not invariably impede intelligence
collection. Indeed, there are numerous examples of cases in which terrorism defendants
in the criminal justice system, represented by counsel, have provided important intelligence
to the government (see supra text and notes 62, 66). Nor does the absence of counsel
ensure successful intelligence collection.
speedy trial rights, venue, appeals, and other issues. But the

193. While military commission rules impose certain timeframes designed to ensure a speedy trial, they are more flexible than the rules set forth in the federal Speedy Trial Act. Compare 18 U.S.C. §3161 et seq. with U.S. Dep't of Dep., Manual for Mil. Commns 707 (2010); it is not clear that the Sixth Amendment right to a speedy trial applies to military commissions. See generally Barker v. Wingo, 407 U.S. 514 (1972). In habeas proceedings, there are no rules mandating timeframes for the resolution of the case similar to the Speedy Trial Act; any court proceedings are governed by rules adopted by individual judges. Where habeas does not apply, evidentiary issues and procedural rules are governed by administrative procedures. See Detainee Review Board Procedures at Bagram Theater Internment Facility, Afghanistan, attached as an appendix to Brief of Respondent-Appellants, Maajed v. Gates, Nos. 09-5265, 09-5266, 09-5277 (D.C. Cir. Sept. 14, 2009).

194. Federal criminal prosecutions operate under relatively strict rules regarding the location (or venue) in which the prosecution and trial can take place as compared to military commission prosecutions. Where any portion of a criminal offense occurs within the United States, venue is governed by Constitutional and statutory provisions, which require the trial to take place in the federal district where the offense, an element of the offense, or any overt act comprising the conspiracy has occurred. See U.S. Const. art. III, §2, cl. 3; 18 U.S.C. §3237; Fed. R. Crim. P. 18. For extraterritorial offenses, venue lies by statute in the district where the defendant is first brought or arrested or, if an indictment is to be returned prior to the defendant's arrest and return to the United States, in the district of his last known residence (or, if none, in the District of Columbia). U.S. Const. art. III, §2; 18 U.S.C. §3238. Military commissions, on the other hand, do not operate under such restrictions, and so the proceedings can be conducted in geographically convenient locations, domestically or abroad. Habeas proceedings need to be conducted before a federal judge, generally in the district where the detainee is held, but there is greater flexibility with respect to detainees held overseas. Cf. Boumediene v. Bush, 553 U.S. 723, 795-796 (2008) (suggesting that all Guantánamo detainees habeas litigation be transferred to federal district court in D.C. in order to “reduce the administrative burdens on the Government.”).

195. Appellate rights are generally broader in the military commissions system than in the federal courts. In particular, the CMCR has greater flexibility to review factual issues and to set aside convictions based on factual insufficiency than does a federal court of appeals. Under 10 U.S.C. §950o(d), “the CMCR may affirm only such findings of guilty, and the sentence or such part or amount of the sentence, as the Court finds correct in law and fact and determines, on the basis of the entire record, should be approved. In considering the record, the Court may weigh the evidence, judge the credibility of witnesses, and determine controverted questions of fact, recognizing that the military commission saw and heard the witnesses.” By contrast, a federal court of appeals will generally review a jury verdict of guilt by “viewing the evidence in the light most favorable to the prosecution” to determine whether “any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.” Jackson v. Virginia, 443 U.S. 307, 319 (1979). This standard requires “a healthy respect for the trial court’s responsibility ... to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts.” Schriro v. Delo, 513 U.S. 267, 272 (1995) (quoting Jackson, 443 U.S. at 319). The expanded scope of appellate review in the military commissions system creates the possibility for an appellate-level acquittal that is not available to the defendant in federal court (the government cannot appeal an acquittal in the trial court, so the expanded scope of appellate review in this area solely benefits the accused). In addition, the accused in a military commission enjoys a second layer of appeal as of right, to the D.C. Circuit Court of Appeals. 10 U.S.C. §950o(d). In law of war detention, where habeas applies, both sides have the right to appeal an adverse ruling to a federal court of appeals. 28 U.S.C. §2253(a).

196. The chart in Appendix 2 compares the three systems in 14 categories.
comparison highlights some of the most important similarities and differences among our civilian law enforcement, military commissions, and law of war detention authorities. Each of these tools is valuable in its own right. Each has strengths and weaknesses, and whether it is legally appropriate and strategically wise to use any tool in a particular case depends on the circumstances of that case. The choice about which tool to use can be complex and fact-intensive, and should be informed by the judgment of national security professionals who understand the tools and their application in particular contexts.

V. USING OUR AUTHORITIES MORE EFFECTIVELY: THE MIRANDA DEBATE

Whatever their relative strengths and weaknesses today, our civilian and military counterterrorism authorities are evolving and improving, and our experience with them in different contexts will inevitably affect how we choose among them in the future. As I have noted, the military commissions have been substantially reformed twice – from relatively ad hoc tribunals established by presidential order in 2001 to more robust trial mechanisms with extensive rules and procedures as established in the 2006 and 2009 MCAs. I think their credibility and viability have been enhanced as a result, and they will better protect national security, consistent with our laws and our values. As the commissions go forward, we will no doubt be generating more case law and obtaining practical experience that will shape how they operate and how both the government and the public perceives them. Likewise, our use of military detention authority has evolved over time. The executive branch now has much more rigorous policies and procedures for assessing who should be detained as an initial matter than it did in 2001. With respect to Guantánamo detainees, federal courts are also reviewing the lawfulness of detention. We will continue to develop case law in our courts that will inform how we use this authority in the future. This may or may not make detention more difficult, but I think it will make detention more sustainable over time and demonstrate our commitment to the rule of law as we work to protect national security.

The same is true of our use of law enforcement authority. I have explained how our government, after the 9/11 attacks, made major changes to permit closer coordination between, and integration of, our law enforcement and intelligence activities. The DOJ and the FBI were both reorganized and reoriented to reflect these changes and are now more effective in addressing terrorism and other national security threats.197

197. See supra Part I.
While there have been substantial changes since 9/11 in how all of these tools operate, there remains room for improvement. We must be vigilant and creative in assessing how these tools work and how they can be strengthened. For example, there has been recent discussion about Miranda warnings in terrorism cases. Addressing the costs and benefits of Miranda, as well as the public-safety exception to Miranda and the importance of maximizing its use in terrorism cases, will illustrate generally some of the ways in which we can assess our counterterrorism tools and improve how we use them.

To understand Miranda as an operational matter (rather than a legal one), we have to consider the tension between two of the national security values I have discussed: (1) neutralizing the current terrorist threat and (2) gathering intelligence in order to neutralize future terrorist threats.\footnote{As the Supreme Court explained in \textit{Dickerson v. United States}, 530 U.S. 428 (2000), the Miranda rule is a constitutional one, not amenable to change by statute, and has a long historical pedigree in the Court's decisions.}

Prior to Miranda, we evaluated the admissibility of a suspect's confession under a voluntariness test. The roots of this test developed in the common law, as the courts of England and then the United States recognized that coerced confessions are inherently untrustworthy. Over time, our cases recognized two constitutional bases for the requirement that a confession be voluntary to be admitted into evidence: the Fifth Amendment right against self-incrimination and the Due Process Clause of the Fourteenth Amendment.

While [an 1897 decision relying on the self-incrimination aspect of the Fifth Amendment] was decided before [a 1936 decision relying on the Due Process Clause] and its progeny, for the middle third of the 20th century our cases based the rule against admitting coerced confessions primarily, if not exclusively, on notions of due process. We applied the due process voluntariness test in "some 30 different cases decided during the era that intervened between [the 1936 decision] and [a 1964 decision]." Those cases refined the test into an inquiry that examines "whether a defendant's will was overcome" by the circumstances surrounding the giving of a confession. The due process test takes into consideration "the totality of all the surrounding circumstances—both the characteristics of the accused and the details of the interrogation." The determination "depend[es] upon a weighing of the circumstances of pressure against the power of resistance of the person confessing."

We have never abandoned this due process jurisprudence, and thus continue to exclude confessions that were obtained involuntarily. But our decisions in \textit{Malloy v. Hogan} (1964) and \textit{Miranda} changed the focus of much of the inquiry in determining the admissibility of suspects' incriminating statements. In Malloy, we held that the Fifth Amendment's Self-Incrimination Clause is incorporated in the Due Process Clause of the Fourteenth Amendment and thus applies to the States. We decided \textit{Miranda} on the heels of \textit{Malloy}.

In \textit{Miranda}, we noted that the advent of modern custodial police interrogation brought with it an increased concern about confessions obtained by coercion. Because custodial police interrogation, by its very nature, isolates and pressures the individual, we stated that "[e]ven without employing brutality, the 'third degree' or [other] specific stratagems... custodial interrogation exacts a heavy toll on individual liberty and trades on the weakness of individuals." We concluded that the coercion inherent in custodial interrogation blurs the line

\textcopyright 2010 by the author. All rights reserved.
2011] LAW ENFORCEMENT AS A COUNTERTERRORISM TOOL

matter what tool you use — military, intelligence, diplomatic, or law enforcement — you will likely encounter a tension between these two values, and there will come a time when you have to strike a balance.

For example, consider the military context. When our armed forces locate a high-value terrorist abroad on the battlefield, they must make a basic decision about whether to try to kill him or capture him. Relatively speaking, it may be easier to kill than to capture — it often requires less precision and less risk to the forces engaged in the operation. Compared to a capture operation, a kill operation may have a higher chance of success in neutralizing the terrorist. On the other hand, a capture operation, if successful, offers a significantly greater benefit than the kill operation. Both will neutralize the terrorist, but only the capture operation offers the opportunity to interrogate the terrorist and gather intelligence from him. This is something an economist, as well as a soldier, can understand: one approach involves lower risk and lower benefits, while the other approach involves higher risk and potentially higher benefits.199

The risk/benefit framework is also applicable to the Miranda issue. As I have discussed, the general rule is that statements made in response to custodial interrogation in the United States cannot be used by the government to convict a defendant unless he first received a Miranda warning.200 This is simply a fact of life in the criminal justice system. Facing that fact, officials confronting a terrorist in the United States must decide whether to advise him of his rights. Relatively speaking,

between voluntary and involuntary statements, and thus heightens the risk that an individual will not be "accorded his privilege under the Fifth Amendment... not to be compelled to incriminate himself." Accordingly, we laid down "concrete constitutional guidelines for law enforcement agencies and courts to follow." Those guidelines established that the admissibility in evidence of any statement given during custodial interrogation of a suspect would depend on whether the police provided the suspect with four warnings. These warnings (which have come to be known colloquially as "Miranda rights") are: a suspect "has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires.

Id. at 432-435 (citations and footnote omitted). The Court in Dickerson also cited its prior decision in Quarles, see 530 U.S. at 441, and observed: "If anything, our subsequent cases have reduced the impact of the Miranda rule on legitimate law enforcement while reaffirming the decision's core ruling that unwarned statements may not be used as evidence in the prosecution's case in chief." Id. at 443-444. The Court also noted one important advantage of Miranda: "experience suggests that the totality-of-the-circumstances test... is more difficult than Miranda for law enforcement officers to conform to, and for courts to apply in a consistent manner," and where Miranda is satisfied, it will be "rare" for any defendant to be able to persuade a court that his statements were involuntary. Id. at 444.

199. I emphasize that this discussion addresses the question of battlefield strikes solely as an operational matter to illustrate the concept of operational risks and benefits. The legal underpinnings of such strikes are beyond the scope of this article.

200. See supra note 57.
interrogation without Miranda warnings might result in a higher chance of obtaining intelligence (though, as explained above, Miranda warnings do not typically seem to be the key factor in whether we secure the cooperation of the target).\textsuperscript{201} Compared to Mirandized interrogation, therefore, un-Mirandized interrogation may have a somewhat higher chance of success in gathering intelligence. On the other hand, Mirandized interrogation, if it succeeds and the terrorist talks, offers a greater benefit than its un-Mirandized counterpart. Both gather intelligence, but only Mirandized interrogation offers an enhanced ability to neutralize the terrorist by using his statements to support his long-term detention through the criminal justice system.\textsuperscript{202}

In some cases, Miranda warnings may be the difference between detaining a suspected terrorist and being compelled to release him. For example, consider a case in which the government learns through sensitive intelligence sources and methods that a U.S. citizen in the United States is plotting with al Qaeda to engage in terrorist activity here. Because we do not wish to expose these sources and methods, we might not be able to prove in a habeas corpus proceeding that this individual is part of al Qaeda, as we must in order to detain him under the law of war.\textsuperscript{203} He cannot be prosecuted in a military commission because he is a U.S. citizen.\textsuperscript{204} We also currently lack the useable evidence to prove that the individual is guilty of a crime (including a war crime). However, if we interrogate him with Miranda warnings, we may be able to elicit statements from him that will help us prove, for example, that he has received terrorist training overseas,

\footnotesize{201. See discussion supra Part III.A and notes 58-59, 62.}

\footnotesize{202. A Miranda warning is also useful (though not required) in helping the government meet the separate requirement that the accused’s statement be voluntary (which also applies in a military commission, with some limited exceptions discussed in greater detail in Part IV, supra, 10 U.S.C. §§948r(c) & (d)), or is reliable (which applies even in the context of a habeas corpus petition adjudicating the validity of law of war detention, see, e.g., Ashm v. Obama, 696 F. Supp. 2d 1, 8-9 (D.D.C. 2010) (finding that the government “failed to establish that the (twenty-three interrogation reports [of interrogations of petitioner] bear sufficient indicia of reliability’’); Hatim v. Obama, 677 F. Supp. 2d 1, 10 (D.D.C. 2009) (unrefuted allegations of torture “undermine the reliability of the statements made subsequent” to alleged torture); Al Rabiah v. United States, 658 F. Supp. 2d 11, 40 (D.D.C. 2009) (concluding that detainee’s confessions were “not reliable and credible’’)).}

\footnotesize{203. As discussed, federal habeas courts have used their discretion to protect classified information from unauthorized disclosure; federal criminal courts achieve such protection using CIPA; and the 2009 MCA, contains provisions analogous to CIPA, 10 U.S.C. §§949p-1–949p-7. While these mechanisms have proven generally effective in protecting classified information, there will remain some cases in which classified information that is essential to the government’s case cannot be relied upon due to security concerns, because, for example, the substance of key information, or its source, cannot be shared in any form with the petitioner/defendant/accused. In such circumstances, where the government has no alternative way to prove what the classified evidence would show, the government may not be able to make its case. This concern is potentially applicable to all three systems – Article III courts, military commissions, and law of war detention.}

\footnotesize{204. See supra note 156.}
so that we can convict him and ensure he does not pose a threat. In that situation, Mirandized interrogation may be needed to ensure his detention.\footnote{An un-Mirandized interrogation might yield evidence that the terrorist was part of al Qaeda if he was prepared to admit that fact, which could be used to support detention under the law of war, but only a Mirandized statement of terrorist conduct would support detention under federal criminal law where there is no link to al Qaeda or associated forces.}

Seen in this way, the costs and benefits of Miranda warnings should be clear. Indulging the worst assumptions, they may inhibit short-term intelligence collection, but they also may expand detention options. Putting aside any legal and ethical restrictions that may apply,\footnote{Note, however, that the Fifth Amendment is not violated at the time a statement is taken even if without a Miranda warning. A violation occurs only if and when the government attempts to introduce an unwarned custodial statement in a criminal proceeding. United States v. Patane, 542 U.S. 630, 641 (2004) (plurality opinion) (“[v]iolations of the Fifth Amendment occur, if at all, only upon the admission of unwarned statements into evidence at trial.”). Because a Fifth Amendment violation would only occur at the point at which such an unwarned statement is introduced in a criminal case, agents do not expose themselves to liability merely by taking an unwarned statement. Id. at 641 (“Police do not violate a suspect’s constitutional rights (or the Miranda rule) by negligent or even deliberate failures to provide the suspect with the full panoply of warnings prescribed by Miranda.”).} one approach—eschewing Miranda warnings—involves lower risk and lower benefits, while the other approach involves somewhat higher risk and potentially higher benefits. The choice between them, of course, needs to be made by professionals who understand the details of the tactical situation and their own capabilities, as well as the alternatives. There may be exceptional terrorism cases in which we know in advance we do not need the individual’s statements to ensure his detention, and we have an immediate need to collect intelligence. In such a case, a Miranda warning may be an unnecessary risk to take, even after public-safety questioning has been exhausted (assuming it is legally and ethically permissible to dispense with the warning in those circumstances). On the other hand, and more often in our experience, there are terrorism investigations in which we do not know that we can secure detention through a conviction without the defendant’s statements, and no other assured avenues to detain the individual are presently available.\footnote{Determining that someone is eligible for detention under the law of war, particularly in the United States or if the person is a U.S. citizen, can take time. The government’s protocol for such determinations, made public in 2004, requires several agencies to prepare factual summaries and memoranda and an individual determination made by the President. See Declaration of Mr. Jeffrey N. Rapp, Director, Joint Intelligence Task Force for Combating Terrorism, ¶ 7 (describing process by which Ali Saleh Al-Marri was designated as an enemy combatant), redacted unclassified version attached to Respondents’ Supplemental Response to the Court’s Order During the February 27, 2006 Telephone Conference, Al-Marri v. Bush, 04 Civ. 2257 (Mar. 29, 2006); 150 CONG. REC. S2701-S2704 (daily ed. Mar. 11, 2004) (reprinting February 24, 2004 statement of Alberto R. Gonzalez, White House Counsel, before the American Bar Association’s Standing Committee on Law and National Security) (explaining process by which U.S. citizens Jose}
The question, then, is how to maximize the benefits and minimize the costs of *Miranda* in keeping with our values and the rule of law. Obviously, *Miranda* is a constitutional rule, and it cannot be overruled or changed by statute. But the Supreme Court has recognized an exception to the *Miranda* rule. In 1984, in the *Quarles* case, it held that questioning prompted by concerns about public safety need not be preceded by *Miranda* warnings. In other words, you can use a person’s unwarned answers to public-safety questions to support his conviction and resulting incarceration.

In *Quarles*, the Supreme Court found admissible the defendant’s custodial statement to police officers who asked him about the location of a gun in a supermarket where he was apprehended after a chase – even though he had not yet been *Mirandized* – because of the imminent threat to public safety posed by the gun. The Court explained its reasoning for adopting a public-safety exception:

In such a situation, if the police are required to recite the familiar *Miranda* warnings before asking the whereabouts of the gun, suspects in *Quarles’* position might well be deterred from responding. Procedural safeguards which deter a suspect from responding were deemed acceptable in *Miranda* in order to protect the Fifth Amendment privilege; when the primary social cost of those added protections is the possibility of fewer convictions, the *Miranda* majority was willing to bear that cost. Here, had *Miranda* warnings deterred Quarles from responding to [the police officer’s]

Padilla and Yaser Hamdi were designated enemy combatants); Letter from Richard A. Hertling, Principal Deputy Assistant Att’y Gen., Dep’t of Justice, Office of Legi. Affairs, to Sen. Patrick Leahy (July 6, 2007) (providing information as required by Section 1176 of the Violence Against Women and Department of Justice Reauthorization Act of 2005; explaining process for “enemy combatant” determinations regarding U.S. persons or residents). Such a determination cannot be made in real time, as an arrest is taking place, which makes it difficult to know whether law of war detention is available at the time a decision about whether to administer *Miranda* warnings must be made.

210. *Quarles* involved a man who was suspected of rape and who had run into a supermarket to escape the police. When arrested, he had an empty shoulder holster, and without administering *Miranda* warnings the police asked him “Where’s the gun?” In response, he nodded in the direction of some empty cartons and said, “The gun is over there,” which indeed it was. The trial court found a *Miranda* violation and suppressed the statement, but the Supreme Court disagreed. It determined that “there is a ‘public safety’ exception to the requirement that *Miranda* warnings be given before a suspect’s answers may be admitted into evidence.” *Quarles*, 467 U.S. at 655. Applying that exception to the facts before it, the Court concluded, “[a]s long as the gun was concealed somewhere in the supermarket, with its actual whereabouts unknown, it obviously posed more than one danger to the public safety: an accomplice might make use of it, a customer or employee might later come upon it.” *Id.* at 657.
question about the whereabouts of the gun, the cost would have been something more than merely the failure to obtain evidence useful in convicting Quarles. [The police officer] needed an answer to his question not simply to make his case against Quarles but to insure that further danger to the public did not result from the concealment of the gun in a public area.\textsuperscript{211}

The Court went on to state that the “exception will not be difficult for police officers to apply because in each case it will be circumscribed by the exigency which justifies it. We think police officers can and will distinguish almost instinctively between questions necessary to secure their own safety or the safety of the public and questions designed solely to elicit testimonial evidence from a suspect.”\textsuperscript{212}

The question today is how the public-safety exception recognized in \textit{Quarles} should apply in the context of modern terrorism. The threat posed by terrorism today is far more complex, sophisticated, and serious than the threat posed by ordinary violent crime. Al Qaeda and other international terrorist organizations often engage in sophisticated planning for their attacks, design simultaneous or coordinated terrorist attacks in multiple locations with multiple participants, and employ tradecraft that makes such attacks difficult to disrupt or prevent. The harm inflicted on the public by successful attacks can be catastrophic. As a result, there are corresponding arguments that the public safety exception to \textit{Miranda} permits more questioning when it is designed to mitigate the new threat of terrorism.\textsuperscript{213} As the Court noted in \textit{Quarles}, the public-safety exception is justified by an exigent need to protect the public and avoid a greater “social cost” than the loss of a criminal conviction, and its scope is therefore “circumscribed by the exigency which justifies it.”\textsuperscript{214} Where the exigency in question is the danger of bombs on commercial aircraft or other coordinated mass-casualty attacks – as opposed to a loose gun in a supermarket – the public-safety exception should permit broader questioning, as necessary, to protect against the threat. We therefore need to ensure that guidance to and training of our law enforcement professionals appropriately address the public safety exception to \textit{Miranda} and the potential for broader use of the public safety exception in questioning in the counterterrorism context.

\begin{flushleft}
\begin{itemize}
\item \textsuperscript{211.} \textit{Id.}
\item \textsuperscript{212.} \textit{Id.} at 658-659.
\item \textsuperscript{213.} \textit{See, e.g.,} United States v. Khalil, 214 F.3d 111 (2d Cir. 2000).
\item \textsuperscript{214.} \textit{Quarles, supra} note 209.
\end{itemize}
\end{flushleft}
CONCLUSION

Let me summarize the main points of this discussion. First, following 9/11, the United States developed a much more aggressive and effective national counterterrorism strategy, which includes law enforcement along with enhanced intelligence and military operations. Legal, policy, and organizational changes made after 2001 reflect the recognized value of law enforcement as one of several tools for combating terrorism. We should remember that history today.

Second, precisely because we are at war with a lethal enemy, we must remain focused on how best to win. I believe that winning requires a pragmatic, empirical approach — we must do what actually works as long as it is lawful and consistent with our values. This is not the time to abandon counterterrorism tools that have a proven track record out of deference to abstract notions of correctness or suitability. We must go where the empirical data leads. As an empirical matter, the criminal justice system has advanced three important national security goals: disrupting terrorist plots through detection and arrest, incapacitating terrorists through prosecution and incarceration, and gathering intelligence from and about terrorists through interrogation and recruitment of them as cooperating assets.

There is no inherent tension between national security and the criminal justice system. While our criminal justice system has limits, and is not always the right tool for the job, when it is the right tool it has an exceptional success rate. There are indeed rules — such as the requirement for Miranda warnings — that may at times constrain what we can do within the criminal justice system, but I believe the severity of these constraints has often been overstated. We are a nation of laws, and there are legal rules governing all of our counterterrorism options; there are similar tensions whether we are using the criminal justice system, military authorities, or other means.

Acknowledging the costs and benefits of using any of our options does not, however, demonstrate the value of law enforcement to counterterrorism, or how to choose between law enforcement and another approach in particular circumstances. That, as I noted, requires a dispassionate, rigorous and detailed analysis of how different systems actually operate. For the purpose of evaluating the utility of law enforcement for incapacitating terrorists and gathering intelligence, I have tried to offer a systematic comparison of the criminal justice system with comparable tools in the military system — namely, law of war detention and military commissions. I think this comparison shows the advantages and disadvantages of each of these tools.

Third, in part because of the complexity of these choices, we should not enact laws that protect suspected terrorists from our criminal justice system. These national security decisions are far too complex to be made in the
abstract. Rather, Congress needs to ensure that we have the broad authority required to protect the country (subject to appropriate limits and conditions); the Executive needs to provide sound policy guidance to the field; and the national security professionals who are charged with protecting the country – whether military, intelligence, or law enforcement – should be allowed to do their jobs and exercise some discretion based on the authority and policy guidance given to them.

These decisions can be difficult, and the fast-paced operational environment in which our national security professionals work will not always afford time for lengthy deliberation before action must be taken. Therefore, we have to understand that people on the front lines will, at least at the initial stages, use the tools that they have been trained to use. This means that our troops on the battlefield in Afghanistan will be treating individuals they apprehend there as enemy belligerents or otherwise under a law of war framework, subject to any understandings with the Afghan government. Conversely, our FBI agents and other federal and state law enforcement professionals on the front lines here at home have long treated suspected terrorists they apprehend in the United States under a law enforcement framework, albeit one that recognizes the imperative of collecting intelligence from the suspects, and that remains open to law of war options to the extent legally permitted. In areas overseas, outside of theaters of active armed conflict, it is likely that foreign governments will most often continue to apprehend and detain suspected terrorists in the first instance; if it is in the U.S. interest to seek transfer of such individuals to U.S. custody, we may have more time to determine at the outset what tool best serves our national security objectives. Diplomatic and legal constraints will also restrict our choices in this context.

At the operational level, the array of complex choices seems to require some mechanism for interagency notice. In appropriate cases, when a terrorist comes into the sights or hands of one agency, that agency should notify other national security agencies and provide them an opportunity to propose alternative approaches. This could apply, for example, if law enforcement authorities intend to arrest or take custody of certain terrorism suspects, or if an intelligence agency is told that a terrorism suspect is in liaison custody. Each agency will follow its own procedures and best judgment in the meantime, but notice provides an opportunity to identify viable alternatives where they exist without requiring the government to delay while the matter is debated. We have in recent years greatly expanded our interagency coordination, and the existing processes have proven effective, but that does not mean they cannot be improved. One of the keys to such improvement, I believe, is greater understanding of the relative advantages and disadvantages of the available tools and options. I have tried in this article to move towards that goal.
Appendix I

Examples of Intelligence on Terrorist Activities
Obtained Through the Criminal Justice System

The following summaries provide some examples of the wide range of intelligence that the United States government obtained from terrorism targets in law enforcement custody between approximately 1998 and 2010.

These examples are not intended provide an exhaustive account of the extensive intelligence that has been gained from and about terrorism targets by the FBI or other federal law enforcement authorities. The United States government is cautious about making public the results of its intelligence collection efforts for a variety of reasons, including, most importantly, the need to protect the safety of the cooperating sources and their families; the need to protect ongoing operations; and the need to protect classified information from disclosure. Based on a similar rationale, the Department of Justice does not typically disclose or publicly confirm when a defendant has pled guilty based on a cooperation agreement in an ongoing investigation. In addition, due to the mechanics of cooperation and sentencing, law enforcement officials are reluctant to characterize the nature of particular cooperation efforts before the cooperation has run its course and can be properly evaluated. Accordingly, this summary is intended only to illustrate the kinds of intelligence that can be obtained through the criminal justice system, albeit using examples of actual case histories.

This information was compiled during the time that David S. Kris served as Assistant Attorney General for the National Security Division, and he obtained permission to use it from the Department of Justice and the FBI.

The information contained in these case summaries includes some or all of the following, depending on the availability and sensitivity of the information: a brief description of the investigation or circumstances leading to the arrest; the nature and value of the information provided; and the details of conviction, including charges, and the sentence imposed, where applicable. The examples are categorized based on the terrorist organization to which the information provided pertains; within each subject category, the examples are organized roughly chronologically. Some of the names of particular individuals have been withheld for operational reasons.

Al Qaeda

Subject A:

Subject A, an al Qaeda associate, was detained as a material witness in
connection with the 1998 East African Embassy bombings. He lied to a
grand jury, refused to testify in the face of an immunity order, and was
detained on contempt and perjury charges. However, he subsequently
agreed to debriefings with his attorney present and provided information
regarding al Qaeda and Usama bin Laden (UBL). After 9/11, he provided
information about the location of several al Qaeda camps in the area of
Khost, Afghanistan.

Jamal al Fadl:
Al Fadl was one of the first individuals to join al Qaeda and a key al Qaeda
member during the 1990s. In 1996, he walked into a U.S. embassy
overseas and offered to cooperate against al Qaeda. Al Fadl agreed to be
debriefed by the FBI. During those debriefings, he was not provided with
Miranda warnings nor was he represented by counsel. At that time, law
enforcement and the intelligence community knew little about the structure
of al Qaeda. Al Fadl provided valuable intelligence regarding the structure
of the organization, including the fact that al Qaeda had a Shura Council
and sub-committees; in addition, he identified many high ranking members,
and explained al Qaeda's history and philosophy. At the time and for the
next several years, Al Fadl was a premier source of intelligence regarding al
Qaeda. The following details some of the specific information provided by
al Fadl to the FBI:

- From 1987 through 1995, UBL ran the Islamic Army. UBL
  created numerous divisions in the army in order to confuse
governments in the event that a soldier was captured so that the
soldier's participation in the war could not be traced back to
UBL. Each division or cell within the Islamic Army had its
own goals and objectives such as reconnaissance, operations,
and recruiting and it would not go beyond its own specialty.

- Al Fadl identified Mustafa Shalabi from the Al Farooq Mosque
  in Brooklyn as an associate who worked with UBL and who
was potentially involved in recruiting within the United States.
According to al Fadl, as early as 1992, UBL became very
interested in recruiting those with American citizenship.

- He reported that UBL and Abdullah Azzam established a
  "Mektab al Khidmat" or "Service Office" which handled the
documents, distribution and logistics for all mujahideen who
joined the war in Afghanistan. Although the initial reason for
keeping the documents was to notify their families in the event
of their death, over time the records of dead soldiers were used
to falsify travel documents. In addition to forging travel
documents, the office collected background documents such as
high school diplomas and birth certificates that would be used to back up the forged travel documents.

- Al Fadl identified two key individuals responsible for manufacturing false documents.

- He also identified three other UBL or Azzam associates who traveled to New York to meet with Shalabi.

- He explained that he raised funds for UBL in New York and that a substantial amount of money was raised by targeting individuals and stores in Brooklyn. The funds were sent to Pakistan or were used to make travel arrangements for individuals going to Afghanistan to fight.

- Al Fadl detailed the establishment of a camp outside Mogadishu; he reported that Abu Hafs al Masri ) (a future military commander of al Qaeda) and Abu Talha al Sudani went there to provoke various Somali factions against the U.S. presence in Somalia.

- Al Fadl also explained UBL's interest in Islamic jurisprudence that supported his goal that the Americans must be removed from Saudi Arabia.

- According to al Fadl, UBL sent Wali Khan Amin Shah (a/k/a "Osama Asmurai") to the Philippines to set up new camps and Shah worked very closely with UBL. Al Fadl identified Shah as missing fingers on one of his hands; and he said that in 1996, he had been living at a guest house near Peshawar. Al Fadl explained that he knew Shah had recently attempted to carry out an operation that had failed and that some of his associates had been arrested. Al Fadl also identified other associates of Shah. (As explained below in connection with Shah's intelligence, Shah was arrested for his role in the failed 1995 "Bojinka" plot to bomb multiple U.S. commercial airliners over the Pacific.)

- Al Fadl identified a photograph of Sheik Omar Abdel Rahman as well as of another member of his group, who was previously unknown to the FBI. Rahman (a/k/a "The Blind Sheikh") was later arrested in connection with a separate plot to conduct terrorist attacks in New York. He was convicted in 1995 and sentenced to life in prison.

- He also identified photographs of a Sudanese member of the Islamic Army, and Mutawakil, a Saudi member of the Islamic Army who was an Emir in Jalalabad (Afghanistan).
Al Fadl provided physical descriptions and names of individuals who had established a UBL front company. He provided information on a Saudi who owned a relief organization and worked on other projects with UBL, including a UBL front company, "Premium," which was involved in exporting sunflower seeds.

He explained that UBL wanted an Islamic state in Bosnia but believed that it would never happen in Europe. He also identified an associate that UBL sent to Bosnia.

He identified a palm oil business in Malaysia run by Mammad Salim (aka "Abu Hajer al Iraqi"), who was a member of al Qaeda's Shura Council.

Al Fadl was eventually flown to the United States and charged with various terrorism-related offenses in the Southern District of New York. He pled guilty to conspiracy to attack the national defense facilities of the United States (18 U.S.C. § 2155(b)), and conspiracy to transport explosives in connection with attacking the national defense of the United States (18 U.S.C. §§ 371, 844(h)). He continued to provide high quality intelligence on al Qaeda and testified for the government in the 2001 trial regarding the 1998 East African Embassy bombings.

L'Houssaine Kherchtou:
Kherchtou was an early member of al Qaeda in the 1990s and a member of one of the al Qaeda cells responsible for the 1998 East African Embassy bombings. In August 2000, the FBI approached Kherchtou in Morocco. He agreed to waive his Miranda rights and be interviewed by the FBI. Like al Fadl, Kherchtou was an invaluable source of intelligence regarding the structure and membership of al Qaeda at a time when the United States did not have access to other human source intelligence. For example, Kherchtou explained how al Qaeda recruited people; and how they used non-governmental organizations and false passports. He also explained how al Qaeda developed targets, and conducted surveillance and training; provided information on its finances and membership; and identified the weapons used and the vehicles driven. In addition, he identified al Qaeda's principal liaison with a foreign government, and explained the relationship between al Qaeda and Hezbollah.

After approximately one month of debriefing, he was flown to the United States. He was continually debriefed in the United States by the FBI, with his counsel present. Kherchtou pled guilty in the Southern District of New York to conspiracy to kill U.S. nationals (18 U.S.C. § 2332(b)). He continued to provide significant information on al Qaeda, and he testified for the government in the 2001 and 2010 trials regarding the 1998 East African Embassy bombings.
Ahmed Ressam:
Ressam, the so-called “Millennium Bomber,” was arrested in December 1999 as he attempted to enter the United States from British Columbia through Port Angeles, Washington. At the port he provided a fraudulently obtained Canadian passport and a Costco membership card to the customs inspector. He fled on foot after being asked follow-up questions. The inspector located explosives and bomb-making materials in the trunk of the vehicle. Ressam was apprehended after a four-block foot chase. He was provided with written Miranda warnings in French and was read his Miranda rights in French over the telephone by an FBI agent. He immediately invoked his Miranda rights. The FBI agent alerted the customs inspectors that Ressam’s French accent was not that of a French-Canadian as he claimed, but rather of someone from North Africa.

Ressam was convicted in 2000, after a trial in the Western District of Washington, of carrying explosives during the commission of a felony (18 U.S.C. §§ 844(h)(2)); committing an act of terrorism that transcended national boundaries (18 U.S.C. § 2332b(c)); transporting explosives (18 U.S.C. §§ 842(a)(3)(A), 844(a) and (2)); and using a fictitious name for entry into the United States (18 U.S.C. § 1546). He was initially sentenced to 22 years’ imprisonment. After multiple appeals, the Ninth Circuit held, in February 2010, that the 22-year sentence was well below the applicable guidelines range, and remanded the case for re-sentencing to a different district court judge. The Ninth Circuit issued an amended opinion in December 10, 2010. Ressam’s petition for rehearing and petition for rehearing en banc is pending before the Ninth Circuit.

Ressam began cooperating with law enforcement after his trial, providing significant information on al Qaeda’s Khaled terrorist training camp located in Afghanistan and other terrorist subjects. He also testified in the trial in the Southern District of New York in July 2001 of his co-conspirator Mokhtar Haourari. However, Ressam ultimately stopped cooperating, which led to the dismissal of indictments against two subjects and the termination of successful investigative efforts against a number of other targets.

Subject B:
The Northern Alliance captured Subject B in Afghanistan in 2001. He refused to cooperate with U.S. interrogators immediately after his surrender; however, approximately 2 weeks later, he waived his Miranda rights, and the FBI and the Naval Criminal Investigative Service conducted several interviews. In those interviews, he provided detailed intelligence on his actions with the Taliban and his interactions with al Qaeda and Usama Bin Laden, including describing meeting personally with UBL at an al Qaeda poisons training facility near Kandahar, Afghanistan. In addition, he informed the FBI that after the September 11 attacks, UBL and his cadre of bodyguards moved every four hours to avoid capture, and he described the
vehicles that were used in UBL’s convoy. He provided the FBI with information that UBL had plans for additional attacks following 9/11, and might have already dispatched sleeper operatives to attack the United States. He also described in detail the training he had received from al Qaeda as well as the facilitators who aided his entry into training camps and the camp instructors.

Subject C:
Subject C was arrested in early 2002 in the Middle East and ultimately turned over to the United States. He provided substantial intelligence on al-Qa’ida and Jemaah Islamiyah in several months of debriefings with the FBI, including the following:

- He provided detailed information about his meetings with Khalid Sheikh Mohammed (KSM) and Riduan Isamuddin (a/k/a, “Hambali”), who were directing a joint al-Qa’ida/Jemaah Islamiyah plot to bomb U.S. military targets and the U.S. and Israeli embassies in Singapore and the Philippines. Although the plot itself had already been disrupted by the time of his debriefings (several Jemaah Islamiyah members in Singapore were arrested in December 2001), his reporting was the most complete information provided at that time regarding KSM’s role in directing multiple plots against the United States both before and after 9/11.

- Subject C also identified multiple lower level operatives with whom he had been working prior to his arrest; and he provided dates and meeting locations, the names and descriptions of other operatives, and a detailed chronology of the plot in which he was involved.

- He explained to the FBI how he became involved with al-Qa’ida as a teenager, thereby providing important insight into how al-Qa’ida identifies and recruits valuable Western operatives. He described traveling to Afghanistan and attending his first round of al-Qa’ida training in the summer of 2000, telling his family that he was studying in another country. He described in detail the route he traveled to Afghanistan, the guest houses in which he stayed and the names of people with whom he traveled or stayed en route. He also detailed the training he underwent at al Farooqi, a training camp near Kandahar, and described the trainers and other attendees.

- He also identified several people whom he considered “important” in al-Qa’ida, including “Mukhtar” (KSM). He later met and swore bay’at to him.
UBL told Subject C that he had been selected for an outside mission because he had a "clean" western passport and spoke English well. At UBL's instruction, Subject C traveled to Karachi, Pakistan in the summer of 2001, where he stayed with KSM. KSM taught him how to travel on trains and buses, how to book travel tickets, and how to conform to local customs. After a few weeks, KSM directed him to travel to Malaysia to meet with individuals planning operations against the U.S. and Israeli embassies in the Philippines, and to provide them with funding.

Once in Kuala Lumpur, he met an individual who described being in Karachi with KSM on 9/11, who said that the video equipment in KSM's apartment was set to record on the morning of 9/11. Based on this information indicating KSM's apparent foreknowledge, Subject C concluded that KSM had arranged and coordinated the 9/11 attacks. This was one of the earliest pieces of source reporting, prior to KSM's capture, confirming that KSM was the architect of 9/11.

Subject C provided the FBI with the phone numbers and e-mail addresses that he used to contact KSM.

*Ernest James Ujaama:*
Ujaama was involved in a plot to set up a jihad training camp at a farm in Bly, Oregon, and also operated websites for Mustafa Kamel Mustafa (a/k/a, "Abu Hamza" or "Hamza al-Mastri") the former imam of the Finsbury Park Mosque in London, England. In July 2002, Ujaama was arrested in Denver and brought to Seattle. He was Mirandized upon arrest and immediately invoked is Miranda rights. However, he eventually agreed to be debriefed with his attorney present and provided valuable information to law enforcement regarding Mustafa.

Ujaama pled guilty in the Western District of Washington in April 2003, pursuant to a plea agreement, to conspiracy to violate the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705(b). He admitted to conspiring with others to provide support, including money, computer software, technology and services, to the Taliban and to persons in the territory of Afghanistan controlled by the Taliban.

As part of the plea agreement, Ujaama agreed to cooperate with the government in ongoing terrorism investigations for up to 10 years from the date of the agreement. He was sentenced to 24 months' imprisonment. He absconded from supervised release in December 2006 prior to providing testimony. He was arrested in Belize and returned to the United States and is now in custody. He has resumed cooperation and now faces resentencing with a maximum 30 year sentence. In April 2009, Ujaama testified in the
trial of Oussama Kassir, who was charged with a conspiracy in connection with the Bly jihad training camp and with operating numerous terrorist websites in the same indictment as Mustafa. Kassir was found guilty of all 11 counts against him in May 2009, and he received a life sentence, plus 115 years, in September 2009. Ujaama’s testimony was considered instrumental in helping to secure Kassir’s conviction.

Iyman Faris:
The FBI learned about Faris after KSM’s arrest in Rawalpindi (Pakistan) in March 2003. Agents contacted Faris, who was living in Columbus, Ohio, and he agreed to be interviewed. After he initially only provided scant information, the FBI asked him to take a polygraph. Faris then provided additional information that was of interest.

Over the course of FBI interviews conducted between March and May 2003, Faris, who had trained and fought in both Kashmir and Afghanistan in the late 1980s, provided extensive information about al-Qa’ida operations, leaders and its plans for attacks in the United States, including the following:

- He provided detailed information about his close friend and high-ranking al-Qa’ida affiliate Subject G. He identified photographs of Subject G and his son, both of whom, at the time of Faris’s interviews, were at large in Pakistan and being sought by the United States. Faris gave the FBI a lengthy description of Subject G’s personality and habits, including his daily routine, descriptions of vehicles Subject G used to travel around Pakistan, his communication habits and the security measures he employed. For instance, Faris advised that Subject G would communicate by using multiple cell phones. Faris also described several “errands” he had completed for Subject G (and the al-Qa’ida security tradecraft involved), including entering a travel agency in Karachi shortly after 9/11 dressed as a Tabligh Jamaat member to extend the departure date of approximately five airline tickets to Yemen for one month in order to keep five al-Qa’ida members in Pakistan. Significantly, Faris also described his travel with Subject G in the summer of 2000 to an al-Qa’ida safehouse in Kandahar, Afghanistan and then to an al-Qa’ida training camp “between two mountains,” about an hour’s drive from Kandahar. Faris described having lunch with UBL at the camp, and he identified the locations of the safehouse and camp on a map of Kandahar at the request of FBI agents.
- Faris also identified a photo of KSM, who had been captured just weeks before Faris’s interviews, as an al-Qa’ida official
whom Faris met during his lunch with UBL and who was introduced to Faris as "Botci." Faris told the FBI that during this initial meeting, KSM asked Faris about "ultralight" and other "kit" airplanes, and advised Faris that he was interested in using them as some type of "escaping airplane." KSM asked Faris with researching and providing him with additional information on ultralights. Faris admitted that approximately two or three months after this meeting, he printed material regarding ultralights off of the Internet and gave it to Subject G.

Faris also informed the FBI about meeting KSM again in February 2002, in Karachi. After traveling with Subject G to a "money exchange" location in Karachi, where Subject G picked up approximately $250,000 in cash (U.S.D.) and divided it into five bags, Faris accompanied Subject G's son to a house in Karachi where they delivered the money to KSM. Faris told the FBI that during this meeting, KSM asked Faris for information about his job as a commercial truck driver in the United States and was particularly interested in Faris's shipment of airplane cargo containers and his access to airports.

- Faris also provided the FBI with a description of counter-surveillance methods employed by KSM.
- KSM also pressed Faris for information about bringing al-Qa'ida operatives into the United States. KSM asked about the possibility of forging documents such as driver's licenses and social security cards and about bribing officials in the United States.

According to Faris, KSM believed that al-Qa'ida could accomplish attacks within the United States through bribing police officers.

- During this meeting, KSM tasked Faris with obtaining gas cutters to cut tension wires in order to attack and destroy the Brooklyn Bridge (when Faris returned to the United States).
- Faris advised the FBI that KSM instructed him to communicate in code about this project (e.g., to refer to the gas cutters as "gas stations").
- After a polygraph examination, Faris admitted to the FBI that he had conducted internet research about gas cutters and admitted to taking photos of the bridge and other structures around Manhattan.
- Faris also provided the FBI with critical information about links between KSM, Subject G, and Subject G's relatives in the United States as well as about Faris's own contacts with other
potential al-Qa‘ida sympathizers in the United States, allowing the FBI to investigate other possible domestic threats.

- Faris provided information about his contacts with Majid Khan, a detainee held at Guantanamo Bay, who was arrested in Karachi (Pakistan) in March 2003. That information assisted the FBI in fully identifying the domestic threat posed by Majid Khan, who had resided in Baltimore, Maryland from 1996 to 2002, and ensuring that all domestic links to Majid were exhausted.

- Faris informed the FBI that he believed that al-Qa‘ida was attempting to develop a chemical weapon, because in early 2001, Faris was present when Subject G’s son brought a man who was suffering from gas poisoning from testing that “they” had been conducting at Subject G’s house in Karachi.

Faris pled guilty in the Eastern District of Virginia to one count of providing material support to al-Qaeda (18 U.S.C. § 2339B) and one count of conspiracy to provide material support to al-Qaeda (18 U.S.C. §§ 2339B & 371). Later, Faris stopped cooperating with the FBI and sought without success to withdraw his guilty plea. He repudiated all of his prior statements to the FBI and alleged that he had been threatened with “enemy combatant” status. Faris was eventually sentenced to 20 years’ imprisonment (the statutory maximum).

Nuradin Abdi:
In November 2003, Abdi was arrested by Immigration and Customs Enforcement (ICE) after the Joint Terrorism Task Force (JTTF) learned that he was involved in a plot to blow up or shoot up a shopping mall. Upon his arrest he was Mirandized and immediately waived his rights. Abdi was offered a lawyer provided by his family, which he initially declined. Eventually, he agreed to speak to a lawyer who encouraged him to continue cooperating. Through a number of interviews, Abdi provided a tremendous amount of information regarding his travel to Africa to attend a training camp to fight jihad in Kosovo and Chechnya. He also told law enforcement that upon his return to the United States, he conspired with Iyman Faris and another individual, Christopher Paul, to send equipment overseas to al Qaeda and to plot violent acts in the United States.

In June 2004, Abdi was charged with conspiracy to provide material support to a terrorist act, namely, to murder individuals and destroy property overseas (18 U.S.C. §§ 371, 2339A, 956); conspiracy to provide material support to al-Qaeda (18 U.S.C. § 2339B); knowingly and willfully making a false representation to obtain a travel document (18 U.S.C. § 1546); and using a fraudulently obtained travel document to re-enter the
United States from Africa (18 U.S.C. § 1546). He ceased his cooperation after being charged and underwent a court-ordered competency evaluation. He fired his attorney and hired another attorney who disallowed law enforcement access.

Abdi pled guilty in the Southern District of Ohio to one count of material support to terrorism (18 U.S.C. § 2339A). He was sentenced to ten years' imprisonment in November 2007.

**Lackawanna Six:**

Prior to 9/11, these defendants, U.S. citizens from Lackawanna, New York, traveled to and received training in an al-Qaeda training camp in Afghanistan. At the camp, they met UBL, who spoke about attacking the United States. Bin Laden told the defendants that 50 men were on a mission related to such an attack and claimed responsibility for attacking the U.S. embassies in East Africa.

In September 2002, the defendants were arrested. One defendant initially waived his Miranda rights and provided a signed sworn statement, while in Bahrain. Another also provided a signed sworn statement to the FBI prior to his arrest. Three of the defendants had been interviewed by the FBI prior to their arrests and provided false statements. One was interviewed several times before his arrest and was not completely truthful. Approximately six weeks after their arrests, the defendants agreed to proffer, with their attorneys present, which led to numerous debriefings over the next year. In 2003, all of the defendants entered into plea agreements and agreed to continue to cooperate.

The defendants pled guilty in 2003 in the Western District of New York to various offenses: Faysal Galab pled guilty to providing funds and services to al-Qaeda in violation of IEEPA (50 U.S.C. § 1705); and Yahya Goba, Shafal Mosed, Sahim Alwan, Yaseinn Taher and Mukhtar al-Bakri pled guilty to providing material support to al-Qaeda (18 U.S.C. § 2339B), based on their pre-9/11 travel to Afghanistan to train in an al-Qaeda-affiliated camp. They received sentences ranging from 84 months to 120 months' imprisonment. The defendants also provided assistance through testimony in other terrorism prosecutions in the United States, Australia and in military commissions regarding terrorist training camps and al-Qaeda.

**Mohammed Abdullah Warsame:**

Warsame is a Somali national who obtained refugee status in Canada in 1989 and obtained landed immigrant status thereafter. After attending various training camps in Afghanistan from March 2000 through that summer, including one that he called the "camp of Usama bin Laden," Warsame traveled from Pakistan, via London, to Canada. He thereafter entered the United States (he had married a U.S. citizen in 1995). In December 2003, Warsame was approached by the FBI in Minneapolis and
voluntarily submitted to an interview which took place over two days. Warsame agreed to speak to agents after they asked him to “help the United States.”

In these interviews, Warsame, under questioning, eventually admitted that he had traveled to Afghanistan in March 2002 and trained at a camp he referred to as “Abu Massab’s camp.” After several months, he had traveled to “the camp of Usama Bin Laden.” Warsame advised the FBI that in addition to basic training, specialized training was carried out at the camp, including training in the use of anti-aircraft guns, explosives, suicide missions and poisons. He had heard from others that the trainees in the poisons camp were learning how to attack locations by poisoning the air or atmosphere. Warsame also described for the FBI his time at an al Qaeda guest house in Kandahar and work at the al Qaeda clinic there. He told interviewing agents that he had been tasked to teach English to others working at the clinic, and that, while he was there, a goat was shot so that trainees could practice removing bullets. He initially claimed that he decided to leave Afghanistan to see his family, but under questioning, admitted that he had been given permission to leave Kandahar and was provided funds to travel by Abu Hafs al Masri, al Qaeda’s military commander (later killed in a U.S. airstrike). According to Warsame, Abu Hafs wanted him to leave Afghanistan before his Canadian passport expired and did not want him to apply for a new one in Pakistan in order to avoid suspicion. When asked if Abu Hafs expected Warsame to return to Afghanistan once he obtained a new passport, Warsame answered that Abu Hafs told him that if he wanted to come back, it would be good.

During the initial interviews, Warsame reluctantly admitted that he had made contact with individuals whom he had known in Afghanistan when he arrived in London. He also identified another Canadian citizen attempting to return to Canada from Afghanistan. In a subsequent interview, conducted in August 2004, Warsame provided the FBI additional information about his time and associates in London, including his Canadian associate. Based on information Warsame provided about his contacts in London, the FBI was able to conduct additional investigation to identify those associates. FBI agents believe that Warsame had likely been dispatched for operational purposes to the United States. However, any operational activity that he planned to undertake was disrupted by his arrest and statements he made to the FBI.

Warsame eventually terminated the interviews. Sometime after that, he was arrested and indicted for providing material support to al Qaeda (18 U.S.C. § 2339B). Warsame pled guilty in the District of Minnesota to one count of providing material support to al Qaeda (18 U.S.C. § 2339B). In July 2009, he was sentenced to 92 months’ imprisonment with credit for time served. He was removed from the United States to Canada upon his release in October 2010.
Mohammed Junaid Babar:
Babar was involved with Omar Khyam, Momin Khawaja and others who were arrested and charged in the U.K. and Canada in connection with a 2004 plot to bomb soft targets in the U.K. Babar was placed under surveillance upon his return to the United States in March 2004. He was approached by JTTF agents in April 2004 and participated in five days of voluntary debriefings. Agents advised Babar of his Miranda rights shortly after approaching him. Babar waived his Miranda rights and agreed to be debriefed.

Babar was arrested pursuant to a material witness warrant in April 2004. He pled guilty in the Southern District of New York in June 2004, to a five-count information based on his provision of material support to al Qaeda and to a British group.

Over the years, agents have developed a close working relationship with Babar, who is considered one of the most valuable sources of intelligence on al Qaeda. He also provided information on Lashkar-e-Taiba (LET) and Al-Muhajiroun. Babar arranged jihadi training for the U.K. plotters (and others) in July 2003 where they all received training in basic military skills and light weapons training. He also met with Hadi al-Iraqi, then al Qaeda's head of military activities in Afghanistan, on four occasions in January and February 2004.

He has testified in numerous terrorism trials in the U.K. and Canada and was expected to testify against co-conspirator Syed Hashmi in a 2010 trial in the Southern District of New York; however Hashmi pled guilty on the eve of trial. Babar was sentenced to time served on January 4, 2011.

Subject D:
Subject D waived his Miranda rights during overseas interrogations by the FBI in November 2008. He described attending a terrorist training camp and offering himself as a suicide bomber. He participated in rocket attacks on a U.S. military base in Afghanistan in late 2008, and he provided specific information about a possible terrorist target inside the United States.

Subject E:
Subject E waived his Miranda rights and provided information on at least three camps, where fighters received physical education, and firearms and explosives instruction. According to Subject E, he was told by other fighters in the camp that the instructors at one of the camps were al Qaeda members.
Hizbollah

Khalil El Reda:
El Reda provided information on Hizbollah fundraising activities in Los Angeles and Boston. He described money laundering transactions, as well as how funds were collected and forwarded to a charitable organization that was designated by the Department of Treasury’s Office of Foreign Assets Control as a Hizbollah front organization in 2007.

Subject F:
Subject F was a member, former fighter, recruiter and fundraiser for Hizbollah in the United States, and a relative was a Hizbollah chief for a region of Lebanon. Subject F provided information to the FBI regarding the organization. His information was particularly valuable because it addressed the internal workings of the organization, including, for example, information about its structure, the identity of its members, its intent regarding the United States, and its future potential to commit terrorist attacks against the United States or U.S. interests. Subject F confirmed that he was an actual Hizbollah member and provided details on the recruitment, application and vetting process that Hizbollah undertakes. He explained how he was able to illegally enter the United States through a specific country, thereby alerting the FBI to the potential for other Hizbollah members to do the same.

Subject F was charged with conspiracy to provide material support to Hizbollah in U.S. court. He pled guilty and was sentenced to a term of years in prison. Subject F was deported to Lebanon upon completion of his sentence.

Other Groups

Mohammed Rashed:
Rashed was a member of the “15 May” organization, a terrorist organization active in the 1970s and early 1980s whose goals included promoting the Palestinian cause by causing personal injury and economic damage to U.S. and Israeli interests around the world. Rashed was involved in arranging and carrying out bombing missions to further the organization’s goals and he participated in the planning of some of the bombing missions. In August 1982, Rashed, his wife and young child flew from Baghdad to Tokyo. Before leaving the aircraft in Tokyo, Rashed placed an improvised explosive device (IED) made of PETN under the seat cushion of the seat in which he was sitting and pulled the pin to activate the IED. The aircraft continued on from Tokyo to Honolulu, as Pan Am flight 830. When the aircraft was approximately 20 minutes from Honolulu, the
bomb exploded, killing Toru Ozawa, the 16-year old passenger in the seat previously occupied by Rashed, and injuring 15 others.

Investigation into this incident revealed numerous other bombing missions conducted by Rashed and other 15 May organization members in 1980 and 1982. In July 1987, a nine-count indictment was returned against Rashed and two co-defendants in the District of D.C., charging conspiracy to commit assault and damage to property; conspiracy to commit murder; murder; aircraft sabotage; damaging aircraft used in foreign commerce; placing bombs on aircraft; assault; attempted aircraft sabotage and aiding and abetting, in connection with the bombing of Pan Am flight 830, the bombing of the Mount Royal Hotel in London, England, the attempted bombing of an aircraft in Rio de Janeiro, Brazil, and the attempted bombing of a hotel in Switzerland.

Rashed was captured in Greece in 1988. After Greece denied the U.S. extradition request in 1990, Greek authorities initiated a prosecution of him. Rashed was convicted in Greece in 1992 and ultimately sentenced to 15 years' imprisonment. In December 1996, after serving 8½ years of his sentence, he was released and began a trip to Africa. At the request of the United States, he was detained in a third country. The United States obtained custody of Rashed in June 1998, and he was brought here to stand trial on the pending indictment.

Rashed has been debriefed extensively by U.S. investigators and has provided useful information in the investigation into a 1985 bombing of a U.S. aircraft in Europe that killed four American citizens. He has cooperated with German prosecutors investigating the 1982 bombing of a restaurant in Berlin that killed a two-year-old girl, allowing the German authorities to issue an arrest warrant in that case. He has also cooperated with a French request for an interview relating to the bombing of a synagogue in 1980.

Rashed pled guilty in the District of D.C. in December 2002, to the first three counts of the indictment, conspiracy to commit murder (18 U.S.C. § 1117); conspiracy to commit offenses against the United States, including the bombing of Pan Am flight 830 and the attempted bombing of a flight in Rio de Janeiro (18 U.S.C. § 371); and premeditated murder of Toru Ozawa by means of an explosive device (18 U.S.C. § 1111). The plea included an agreement to cooperate. In exchange for the plea, the prosecutors agreed to recommend a release date of March 2013. In March 2006, Rashed was sentenced to an additional seven years.

**Virginia Jihad:**
The Virginia Jihad case involved a number of individuals who attended the Dar al-Arqam Islamic Center in Falls Church, Virginia, and who participated in paintball and paramilitary training with the encouragement of Ali Al-Timimi, a speaker and spiritual leader at the Center. Soon after 9/11, Al-Timimi encouraged the defendants to go to Pakistan to receive
military training from LET in order to be able to fight against American troops soon expected to arrive in Afghanistan. Four of the defendants traveled a week later and attended an LET camp in Pakistan. Another defendant assisted an LET operative, Mohammed Ajmal Khatt, in obtaining high-tech equipment for LET. This conduct occurred after LET had been designated a foreign terrorist organization.

In early 2003, one of the defendants agreed to six weeks of voluntary debriefings with the FBI. This defendant was later arrested and read Miranda warnings which he waived, and he continued to cooperate. The other defendants were arrested in the months that followed.

In June 2003, 11 defendants were indicted in a 41-count indictment. Four defendants agreed to cooperate and have provided valuable information against their co-defendants who trained at LET camps, including providing testimony in several trials.

Subsequent indictments of two additional defendants, as well as one indictment of a previously-acquitted defendant for perjury, providing false statements, and obstruction of justice, led to three additional convictions. In total, the Virginia Jihad investigation has resulted in the conviction of 12 defendants in the United States, the most in any single terrorism case since 9/11. Those found guilty of charges brought by this investigation have received sentences ranging from approximately four years to life imprisonment.
<table>
<thead>
<tr>
<th>General Procedural Rights for Defendant/Accused/Petitioner</th>
<th>Military Commissions</th>
<th>Law of War Detention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greatest procedural protections.</td>
<td>Most of the rights mandated in federal courts are also required here.</td>
<td></td>
</tr>
<tr>
<td>Full panoply of constitutional rights, including, <em>inter alia</em>, 4th Amendment (search and seizure; probable cause; speedy presentment); 5th Amendment (due process; double jeopardy; exculpatory evidence); 6th Amendment (speedy and public trial; petit jury; confrontation, including right to be present, confront witnesses, compel witnesses; qualified self-representation); Presumption of innocence; notice of charges; guilt must be proven beyond a reasonable doubt; impartial decision-maker; procedures for selection of jurors; Federal Rules of Evidence apply (including limitations on admissibility of prior acts, prejudicial evidence, and hearsay); Unanimous jury of 12 required for verdict; Appeal as of right to federal appeals court; de novo appellate review on facts and de novo review on legal issues; Constitutional and statutory venue requirements apply to limit location of trials.</td>
<td>Some notable differences [in addition to those listed in greater detail below]: Rules on admissibility of hearsay are broader than in federal court but still limited (note this is of potential benefit to both government and accused); Speedy trial rules are not as rigid as those codified in federal Speedy Trial Act (although there may still be constitutional issues); No unanimous jury requirement (2/3 of jury) for conviction; in non-capital cases, minimum of 5 members required on jury; Jury consists of military officers; Two layers of appeal: (1) Court of Military Commission Review, which has greater flexibility to review factual issues (in addition to legal review), and to conduct a rehearing; and then (2) D.C. Circuit, which conducts deferential review of facts and de novo review of legal issues; No venue restrictions as in federal criminal trials so trials can take place in geographically convenient locations, domestic or abroad.</td>
<td>Fewest procedural protections. Where habeas applies: Supreme Court has recognized that standards and procedures to be applied must account for the special circumstances of wartime detention, and left open the contours of the substantive and procedural law for lower courts to shape in a common law fashion; Detainee has a right to an adversarial proceeding before a federal judge although it is possible there can be some delay before this right attaches; Generally, at a minimum, detainee has right to unclassified evidence upon which detention is based, to respond to that evidence, and to &quot;exculpatory&quot; evidence; Procedural rules are based on the discretion of the judges and broadly favor admission; hearsay is admissible; assessment of weight given hearsay is very fact dependent; Appeal as of right to federal appeals court, with deferential review of facts and de novo review of legal issues; Proceedings need to be conducted before a federal judge, generally in district where detainee is held, though different rules apply with respect to detainees held overseas (for example, all of the Guantanamo habeas litigation is conducted in federal court in D.C.). Where habeas does not apply: Procedural protections are based solely...</td>
</tr>
<tr>
<td>FEDERAL COURTS</td>
<td>MILITARY COMMISSIONS</td>
<td>LAW OF WAR DETENTION</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td><strong>SCOPE &amp; WHO MAY BE DETAINED</strong></td>
<td><strong>Cannot charge a U.S. citizen;</strong>&lt;br&gt;<strong>Must be an “alien” and an “unprivileged enemy belligerent” — that is, an individual who has engaged in or has purposefully and materially supported hostilities against the U.S. or its coalition partners; or was part of al Qaeda, Taliban or associated forces at the time of commission of offense;</strong>&lt;br&gt;<strong>Does not currently include individuals who are part of or supporting terrorist groups not affiliated with al Qaeda, Taliban, or associated forces (e.g., Hamas or Hezbollah).</strong></td>
<td><strong>Citizenship and alienage not generally relevant (although location/circumstances of capture may be relevant — see below);</strong>&lt;br&gt;<strong>Must be within ambit of AUMF — which the government interprets as informed by law-of-war principles to authorize detention of those who are part of, or who substantially supported, Taliban, al Qaeda, or associated forces that are engaged in hostilities against the United States or its coalition partners;</strong>&lt;br&gt;<strong>Does not include individuals who are part of or supporting terrorist groups not affiliated with al Qaeda, Taliban, or associated forces (e.g., Hamas or Hezbollah).</strong></td>
</tr>
<tr>
<td><strong>REQUIRED PROOF</strong></td>
<td><strong>Offense must be punishable by MCA or law of war (or two UCMJ offenses);</strong>&lt;br&gt;<strong>32 MCA offenses (covering many but not all terrorism-related offenses including hijacking, murder, terrorism, material support);</strong>&lt;br&gt;<strong>There is some risk that courts may reject material support and conspiracy charges (at least to the extent they are as broadly construed as in the federal criminal code) based on ex post facto or other concerns;</strong>&lt;br&gt;<strong>Does not cover other federal criminal code-type offenses (e.g., immigration)</strong></td>
<td><strong>No offense needs to be charged;</strong>&lt;br&gt;<strong>However, must be within AUMF (and, where habeas applies, will have to show evidence of this to an Article III court).</strong></td>
</tr>
</tbody>
</table>

1. This discussion does not address any independent constitutional power that may exist with respect to detention.
<table>
<thead>
<tr>
<th><strong>EVIDENTIAL BURDEN</strong></th>
<th><strong>FEDERAL COURTS</strong></th>
<th><strong>MILITARY COMMISSIONS</strong></th>
<th><strong>LAW OF WAR DETENTION</strong></th>
</tr>
</thead>
</table>
| o Government must prove accused is guilty of the crimes charged beyond a reasonable doubt;  
 o Presumption of innocence;  
 o Evidence is admissible consistent with Federal Rules of Evidence. | | o Government must prove accused is guilty of the crimes charged beyond a reasonable doubt;  
 o Presumption of innocence;  
 o Evidence is admissible consistent with 2009 MCA and 2010 Manual on Military Commissions. | Where habeas applies:  
 o Government must prove detention is authorized under AUMF; district courts have generally required proof by a preponderance of the evidence, a standard which the D.C. Circuit has upheld as constitutionally sufficient;  
 o Rebuttable presumption in favor of the government as to authenticity of the evidence (at least based upon District Court Case Management Order governing habeas cases);  
 o Evidentiary rules are generally within individual judge’s discretion (guidance from D.C. Circuit suggests rules should be broadly applied in favor of admissibility);  
 o District judges have thus far reviewed evidence rigorously (although different judges have evaluated similar evidence differently in some contexts).  
 Where habeas does not apply:  
 o Governed solely by administrative procedures. |
| **DURATION OF CONFINEMENT** | | o Temporal limitation is length of sentence, regardless of whether conflict exists or the nature of the conflict. | o Temporal scope is indeterminate: authority to detain will end when conflict ends; when hostilities end, international law requires prompt repatriation;  
 o May be difficult to determine when that is, but should endure at least while U.S. troops are engaged in combat;  
 o Even if conflict is still ongoing in some |
<table>
<thead>
<tr>
<th><strong>FEDERAL COURTS</strong></th>
<th><strong>MILITARY COMMISSIONS</strong></th>
<th><strong>LAW OF WAR DETENTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SENTENCES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(NON-CAPITAL)</td>
<td>o Based on statutorily-established maximums and, in some cases, mandatory minimums;</td>
<td>o Imposed by members of the panel, not judge;</td>
</tr>
<tr>
<td></td>
<td>o Determined by judge;</td>
<td>o No Sentencing Guidelines or mandatory minimum sentences;</td>
</tr>
<tr>
<td></td>
<td>o Judge's discretion is further guided by Sentencing Guidelines;</td>
<td>o Panel can impose any sentence as long as it does not exceed statutory maximum or any limitation imposed by Secretary of Defense;</td>
</tr>
<tr>
<td></td>
<td>o Can have lengthy sentence, so defendant could be detained even if conflict is deemed to have ended.</td>
<td>o Can have lengthy sentence, so accused could be detained even if conflict is deemed to have ended.</td>
</tr>
<tr>
<td><strong>DEATH PENALTY</strong></td>
<td>o Imposed by unanimous jury of 12;</td>
<td>o Imposed by unanimous jury of indeterminate number (minimum of 12 unless &quot;reasonably unavailable ... because of physical conditions or military exigencies,&quot; but there must be at least nine.);</td>
</tr>
<tr>
<td></td>
<td>o Can clearly be imposed after a guilty plea;</td>
<td>o Currently, it is unclear whether commission judges would permit death penalty to be imposed after a guilty plea under applicable law, though legislation has been proposed on that issue;</td>
</tr>
<tr>
<td></td>
<td>o Established procedures exist for deciding to seek death penalty, for assigning &quot;learned&quot; counsel, and for conducting sentencing phase of capital trial.</td>
<td>o Questions still need to be resolved about availability, resources, and standards for defense counsel in death penalty cases (possibly adding to litigation issues).</td>
</tr>
<tr>
<td><strong>IMPACT OF LOCATION OF CAPTURE (e.g., APPLICATION IN THE)</strong></td>
<td>o No impact – captures within or outside U.S. can be charged.</td>
<td>o Does not present a bar to triability of offense per se; however, detention authority could be impacted if capture is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Courts have been divided on whether an individual – particularly a U.S. citizen or legally present alien – who is captured</td>
</tr>
<tr>
<td></td>
<td>Federal Courts</td>
<td>Military Commissions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>United States</td>
<td></td>
<td>within U.S. (see LOW detention box).</td>
</tr>
<tr>
<td>Admissibility of Confessions</td>
<td>○ In order to use defendant’s statements against him, statements must have been preceded by Miranda warning, unless certain exceptions apply (e.g., public safety); ○ Statements must also be voluntary (including no torture/CID elicited confessions); ○ “Fruits” of involuntary statements are generally barred (fruits of a voluntary but un-Mirandized statement are not barred).</td>
<td>○ No need for Miranda warning; ○ Statements must be reliable and voluntary, with a limited exception to voluntariness requirement for statements made at point of capture during a military operation; ○ Torture/CID elicited confessions are barred; ○ While “fruits” of torture/CID elicited confessions are generally barred under the 2010 Military Commissions Manual, there are exceptions that may permit such evidence to be introduced under broader circumstances than is permitted in federal courts; ○ Unclear how rules will operate in practice, and there is a risk that courts may find that due process requires exclusion of “fruits” of unlawfully-obtained statements beyond that contemplated by the rules.</td>
</tr>
</tbody>
</table>
## Appendix 2 to Article by David S. Kris

| FE
dERAL COURTS | MILITARY COMMISSIONS | LA
W OF WAR DETENTION |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right to Counsel</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o Sixth Amendment right to counsel attaches when adversary judicial process begins – usually when individual first appears in court on charges or at indictment, whichever occurs first – and includes right to presence of counsel at any interrogation (concerning offenses for which he is charged);</td>
<td>o No right to counsel upon being taken into custody (timing of right to counsel depends on applicability of habeas and when right attaches if habeas applies – see LOW box);</td>
<td>o Right to counsel is based on right to habeas.</td>
</tr>
<tr>
<td>o &quot;Offense-specific&quot; right, so statements not concerning charged conduct would be admissible regardless of presence of counsel;</td>
<td>o 2009 MCA requires that qualified military defense counsel be assigned &quot;as soon as practicable&quot;;</td>
<td>Where habeas applies:</td>
</tr>
<tr>
<td>o Right to counsel includes right of defendant who does not require appointed counsel to choose counsel;</td>
<td>o Right to civilian counsel of own choosing at no expense to government;</td>
<td>o Individual detained must be afforded access to counsel at some point, at least for the purpose of contesting the facts the government asserts to justify detention;</td>
</tr>
<tr>
<td>o Government must present defendant in court without unnecessary delay after arrest; at that appearance individual will have right to counsel;</td>
<td>o Latest such a right could attach is at the time that charges are referred, although accused may be provided counsel when charges are sworn, if not before.</td>
<td>o It is not clear when this right attaches. It may be different within the United States as compared to areas outside the United States.</td>
</tr>
<tr>
<td>o Government may not delay presentment solely for purpose of law enforcement questioning;</td>
<td>o Denial of individual’s access to counsel for an extended period may raise independent due process questions, even before the right to counsel attaches at presentment.</td>
<td>Where habeas does not apply:</td>
</tr>
<tr>
<td>o Denial of individual’s access to counsel for an extended period may raise independent due process questions, even before the right to counsel attaches at presentment.</td>
<td></td>
<td>o There is no right to counsel; however, administrative procedures require a personal representative be appointed within a specific time period to assist detainee with administrative hearing.</td>
</tr>
</tbody>
</table>

<p>| INCENTIVES TO PROVIDE INFORMATION | | |
| o Established procedures that are well-known and understood by all parties provide incentives to cooperate through proffer agreements, cooperation plea agreements, pre-sentencing motions under the Sentencing Guidelines or post-sentencing motions permitting judge to reduce sentence based on | o Mechanism analogous to a plea/cooperation agreement under which party may negotiate pre-trial agreement including applicable sentencing range; | o No regular, well-understood and enforceable mechanism for balancing conditions and duration of confinement against cooperation; |
| | o Use of cooperation plea agreements is not as well-tested as in federal court; | o At least for a certain amount of time, it may be possible to alter conditions of confinement; preclude involvement of attorney; and segregate detainee to |</p>
<table>
<thead>
<tr>
<th>INTERNATIONAL</th>
<th>FEDERAL COURTS</th>
<th>MILITARY COMMISSIONS</th>
<th>LAW OF WAR DETENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>COOPERATION</td>
<td>&quot;substantial assistance&quot; that defendant provided to the government; Generally not possible for interrogator to alter conditions of confinement; preclude involvement of attorney; or segregate detainee to facilitate intelligence collection to same extent as in law of war detention.</td>
<td>used as parameters for any negotiations; No extensive practice of post-conviction, pre-sentencing cooperation or an established post-sentencing cooperation mechanism; Sentencing is not done by an individual judge but by the commission, so impact of cooperation may not be as predictable; Prior to the initiation of military commission charges, it may be possible to alter conditions of confinement; preclude involvement of attorney; and segregate detainee to facilitate intelligence collection; Once military commission prosecution starts it is unclear to what extent conditions of confinement can be altered; however, the timing of when the prosecution is initiated after the initial custody is in the government's control.</td>
<td>facilitate intelligence collection; Where habeas applies, at some point an attorney would likely become involved, and a court hearing take place, reducing the availability/impact of segregation.</td>
</tr>
<tr>
<td>Well-respected internationally; Established formal legal mechanisms allow transfer of suspects to the U.S. for trial and for provision of information to assist law enforcement investigations (i.e., extradition treaties and MLATs); Other countries are comfortable with these procedures as well as other informal mechanisms; Some key allies will not provide assistance for cases in which death penalty is sought; Some countries might prefer alternate forum if it would permit their assistance to be kept secret.</td>
<td>Many allies not willing to extradite to or provide assistance in connection with military commission proceedings; Some extradition treaties explicitly forbid extradition for proceedings in &quot;extraordinary&quot; courts; Some key allies will not provide assistance for cases in which death penalty is sought; Some countries might prefer to assist military commissions rather than federal courts if it is more likely that assistance can be kept secret in the former.</td>
<td>Many allies not willing to extradite to or provide assistance in connection with habeas proceedings to support law of war detention; Some extradition treaties explicitly forbid extradition for proceedings in &quot;extraordinary&quot; courts; Some countries might prefer to assist law of war detention rather than federal courts if it is more likely that assistance can be kept secret in the former.</td>
<td></td>
</tr>
<tr>
<td><strong>PROTECTION OF CLASSIFIED INFORMATION AND PUBLIC PROCEEDINGS</strong></td>
<td><strong>FEDERAL COURTS</strong></td>
<td><strong>MILITARY COMMISSIONS</strong></td>
<td><strong>LAW OF WAR DETENTION</strong></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>CIPA, and interpretive case law, governs use of classified information; CIPA permits government to provide defense a substitute for the actual classified information, such as statement of relevant facts or summary if the court finds that the substitute will provide the defendant substantially the same ability to make his defense as would disclosure of the specific classified information; Federal court trials are presumptively open to the public (constitutionally required as a general matter); Can only be closed in limited circumstances; Proceedings are accessible to all who want to watch in person and/or report about them, subject to logistical constraints (but not televised).</td>
<td>Procedures for handling classified information are modeled on CIPA; fundamental procedures are very similar although 2009 MCA makes some rules explicit that have developed in federal court through judicial interpretation and practice and clarifies others; Military commission judges are required to view federal court precedent as authoritative unless the text of the MCA specifically requires a different result; Military commissions are presumptively open to the public; However, can be closed in potentially broader circumstances than a federal court trial (judge must still make a determination that closure is necessary to protect national security/physical safety of a participant; accused may argue constitutional standard applies); Accused is not excluded even if testimony warrants closure of the courtroom to the general public; There is a 45-second delay of the broadcast of statements to permit the airing of classified information to be blocked in certain cases (and public is not in same room as trial); Jury consists of military officers, who may have more familiarity in dealing with classified information than many civilians.</td>
<td>Where <strong>habeas applies:</strong> Individual judges set procedures and have more flexibility to shield classified information from the detainee; Courts have, however, typically required that the government provide at least petitioners' cleared counsel the classified information it is relying upon to justify detention or that is &quot;exculpatory,&quot; even if only in summary. In rare cases the government has sought exceptions to disclosure, particularly for marginally &quot;exculpatory&quot; information; Judges have not considered evidence on the merits that the detainee's counsel has not been shown in some form; Although theoretically open to the public, as a practical matter vast majority of district court proceedings are closed to protect classified information; Petitioner does not have right to be present at hearing and usually is not, so closed proceedings involve only judge, counsel, and other court personnel; Arrangements are made for petitioners to listen from Guantanamo to unclassified opening statements, and they often testify in their cases via video link; Appellate proceedings have required the filing of public briefs (in which classified material is redacted) and oral arguments have generally been open to the public, with the court holding additional closed sessions when necessary</td>
<td></td>
</tr>
<tr>
<td>Where <strong>habeas does not apply:</strong> Subject only to administrative rules.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERTAINTY/FINALITY OF SYSTEM</td>
<td>FEDERAL COURTS</td>
<td>MILITARY COMMISSIONS</td>
<td>LAW OF WAR DETENTION</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Clean/established rules and extensive experience/precedents and practice;</td>
<td>○ Clean/established rules and extensive experience/precedents and practice;</td>
<td>○ Statutory basis for authority and rules (2009 MCA);</td>
<td>○ Statute (AUMF) and case law provide basis for authority;</td>
</tr>
<tr>
<td>Most predictable and well-established system, providing the greatest certainty that a successful proceeding will lead to long-term detention that will be sustained upon appeal;</td>
<td>○ Most predictable and well-established system, providing the greatest certainty that a successful proceeding will lead to long-term detention that will be sustained upon appeal;</td>
<td>○ Lacks established precedents and practice on many issues;</td>
<td>○ While the government's authority to detain under the AUMF is established and is widely accepted (at least by U.S. courts), questions exist about the contours of that authority (especially for individuals apprehended in the United States);</td>
</tr>
<tr>
<td>Well accepted and respected internationally.</td>
<td>○ Well accepted and respected internationally.</td>
<td>○ Subject to constitutional challenges to the system as a whole as well as extensive litigation as to how statute/rules will apply (given uncertainty and novelty of procedures) in a given case;</td>
<td>○ Where habeas applies, substantial questions have been litigated about the procedural/evidentiary rules that are applicable to habeas proceedings;</td>
</tr>
<tr>
<td>○ There is some risk that courts may find that new procedural safeguards and rules in the 2009 MCA and 2010 Military Commissions Manual do not satisfy all due process concerns or that other constitutional safeguards apply;</td>
<td>○ Success rate for the government has been significantly lower in habeas cases than is traditionally achieved in criminal prosecutions;</td>
<td>○ There is also some risk that courts may reject certain substantive offenses;</td>
<td>○ Courts have not definitively resolved where habeas applies, beyond the U.S. and locations within the effective control of the U.S. such as Guantanamo;</td>
</tr>
<tr>
<td>○ Not yet as well-accepted internationally.</td>
<td>○ Not yet as well-accepted internationally.</td>
<td>○ Not yet as well-accepted internationally.</td>
<td>○ Not yet as well-accepted internationally.</td>
</tr>
</tbody>
</table>