A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security

James Burch

SUMMARY

"The safest place in the world for a terrorist to be is inside the United States. . . . As long as terrorists don't do something that trips them up against our laws, they can do pretty much all they want."

Brent Scowcroft, former National Security Advisor[1]

Several paradigms were altered on 9/11. The U.S. intelligence community, largely focused on state actors, now faced the threat posed by elusive terrorists. The community also had to address the asymmetry posed by the terrorists' use of unconventional and relatively unsophisticated methods to create loss of life and damage – a more complex intelligence task. Lastly, due to terrorist disregard for national borders, laws, and transnational financing, the United States had to change its concept of foreign versus domestic intelligence.[2]

The area of domestic intelligence raises several issues. First, law enforcement and intelligence operate in different worlds – one seeks to prosecute, the other to gather information.[3] Second, with the development of multiple state fusion centers and the creation of additional organizations focused on intelligence, there is a corresponding increase in bureaucratization. This adds to the challenge of sharing information. Lastly and perhaps most importantly, there are issues concerning the protection of civil liberties and effective oversight.

The challenge in developing a viable domestic intelligence capability for the United States centers on how to organize these capabilities optimally within the larger U.S. intelligence framework, how to ensure streamlined information sharing between foreign intelligence and the multitude of law enforcement agencies, and how best to implement oversight mechanisms to protect civil liberties and ensure accountability of intelligence operations. *Organizational mechanisms*, *information sharing*, and *oversight* are the three critical components to instituting an effective domestic intelligence capability.

One of the proposed constructs to meet these organizational and information sharing challenges is to create a domestic intelligence agency. The United States is unique among Western or highly industrialized countries in that it does not possess one. This paper examines the feasibility, suitability, and acceptability of instituting a domestic intelligence agency in the United States from the viewpoint of organization, information sharing, and oversight. It will assess the domestic intelligence organizations of three countries that possess liberal democratic institutions – the United Kingdom's Military Intelligence 5 (MI5), the Australian Security Intelligence Organisation (ASIO), and India's Intelligence Bureau (IB) – to determine their relative effectiveness in countering terrorism, identify their strengths and shortfalls, and determine applicable policy recommendations for the United States.

Specific criteria are used to establish a measure of assessment for a domestic intelligence agency. In this case, the criteria are derived from the Geneva Centre for the Democratic

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**26**	

Control of Armed Forces (DCAF), which partners with countries to promote governance and determine recommendations that promote government reform. Examples of some criteria are the subordination of intelligence to national laws, effective coordination, and oversight.

Examining countries with similar democratic institutions, threats, and (in the case of Australia and India) geographic scope will result in identifying key factors for instituting an effective domestic intelligence capability for the United States. This examination will also determine whether current intelligence reform policies are targeting perceived intelligence shortfalls and offer additional recommendations. It will also determine whether the establishment of a domestic intelligence agency is feasible, acceptable, and suitable to meeting the asymmetric threats of the 21st Century.

INTRODUCTION

Al Qaeda conducted a devastating strike on 9/11 by using airliners as weapon of mass destruction (WMD). In terms of scale, they incurred a relatively small cost to create billions of dollars worth of damage.[4] The psychological impact was also devastating and prompted a massive response and reorganization of the U.S. government to combat this threat.[5] Part of this reorganization was a close examination of the Federal Bureau of Investigation (FBI). A Congressional inquiry into 9/11 revealed several FBI shortcomings:

- "The FBI's decentralized structure and inadequate information technology made the Bureau unable to correlate the knowledge possessed by its components. The FBI did not gather intelligence from all its many cases nation-wide to produce an overall assessment of al Qaeda's presence in the United States."
- "Many FBI field offices had not made counterterrorism a top priority and they knew little about al Qaeda before September 11."
- The FBI also did not inform policymakers of the extent of terrorist activity in the United States. "Although the FBI conducted many investigations, these pieces were not fitted into a larger picture."[6]

These findings highlighted a domestic intelligence gap and, as a result, have led to several larger governmental initiatives and internal FBI reforms. Another organizational alternative is to create a domestic intelligence agency to focus solely on domestic intelligence and collection. Supporters of a domestic intelligence agency have proposed this alternative as the best method to effectively address the domestic intelligence gap. In attempting to address this gap, however, there are additional issues. First, there are opposing viewpoints as to whether the domestic intelligence apparatus should remain within and tied to the FBI versus establishing it as an independent entity. Second, the creation of another bureaucracy raises concerns about the effectiveness of information sharing. Third, an increased focus on domestic intelligence leads to concerns about civil liberties and oversight. Examining the domestic intelligence structures of the United Kingdom, Australia, and India in terms of these three issues can assist in determining the applicability of those structures and offer implementation considerations for the United States.

Advocates for a separate domestic intelligence agency point to several advantages. The first is a symbolic one: the creation of such an agency would emphasize the government's commitment to preventing another catastrophic attack.[7] As Mark

Lowenthal states, "several issues spill over into the domestic realm – economics, narcotics, crime, and terrorism – thus curtailing the activities of much of the intelligence community . . ."[8] A domestic intelligence agency would also focus directly on these domestic-foreign terrorism nexus' issues and afford greater precision to developing and categorizing the domestic threat. Creating an agency strictly focused on this mission could more directly address the domestic intelligence gap as compared to the higher organizational and bureaucratic changes that have been implemented since 9/11.

Second, there is inherent competition between law enforcement and intelligence for resources and focus. Harry Ransom highlighted this competitive tension when referring to CIA intelligence and operations: "The ill advised marriage of intelligence collection-analysis-estimates with covert action has further complicated role theory."[9] Advocates for a domestic intelligence agency argue that the FBI's intelligence function will always take a secondary role to its law enforcement responsibilities due to the focus on "making cases" and the preponderance of the FBI's leadership coming from law enforcement.[10] Combining two missions that operate in different worlds and possess different challenges under one organization contributes to operational ineffectiveness.

Lastly, it is much easier to recruit, perform undercover work, and take advantage of the loyal Muslim base in the United States.[11] As one FBI official noted before a Congressional inquiry, "foreign governments often knew more about radical Islamist activity in the United States than did the U.S. Government because they saw this activity as a threat to their own existence."[12] The development of a domestic intelligence baseline to categorize the terrorist threat in terms of cells, planning efforts, and underlying support networks would directly support investigatory efforts. For the advocates, a renewed focus by a domestic intelligence agency dedicated to developing these intelligence resources in the United States would directly support prevention efforts.

Despite the advantages, there is also considerable opposition. Opponents counter that the addition of another organization adds another layer of bureaucracy, making it harder to overcome the already obscured relationship between law enforcement and intelligence.[13] Creating another agency, while having the merit of focusing on intelligence issues, does not address the larger problem of information sharing outside of its organization.[14] As Eric Taylor states, "added bureaucracies will only cause agile terrorist groups glee as they outmaneuver sluggish government attempts to counter them."[15]

There is also the potential abuse of civil liberties and danger of politicization. U.S. intelligence agencies historically have had limited roles in internal security.[16] Letting an organization pursue an aggressive domestic intelligence agenda could lead to the domestic spying abuses similar to those of the 1950s and 1960s.[17] The potential for such abuse will also increase the scrutiny of the executive branch, which could lead to a backlash similar to the Church and Pike Commission recommendations.[18] There is also the danger of politicization. As Ransom asserts, ". . . politicization is inherent in the production of intelligence because information is crucial to gaining and preserving political power."[19] A domestic intelligence agency has the unique potential of becoming politicized. As Ransom further states, the CIA was insulated from partisan politics from 1947 to 1967 because, "a foreign policy consensus prevailed, secrecy normally expected by an intelligence agency was maintained and congressional knowledge and monitoring of intelligence operations was very limited."[20] Those sets of circumstances do not exist today.

The arguments for developing a domestic intelligence agency center on its prevention activities, the organization's unity of purpose, and the recruitment of intelligence sources. The reasons for not implementing are the additional layers of bureaucracy that do not facilitate information sharing, the potential abuse of civil rights, and the danger of politicization. The challenge and key task is to determine how to organize domestic intelligence efforts, how to facilitate information sharing, and how to protect against potential abuses in the U.S.

Democracies, by their nature, are faced with a conflicting dilemma regarding terrorism. As Benjamin Netanyahu, the former Prime Minister of Israel, states:

> The governments of free societies charged with fighting a rising tide of terrorism are thus faced with a democratic dilemma: If they do not fight terrorism with the means available to them, they endanger their citizenry; if they do, they appear to endanger the very freedoms which they are charged to protect.[21]

This dilemma lies at the center of the public debate. Richard A. Posner, a noted jurist, identifies two issues. The first is where to draw the line between security and liberty; the second is which controls are necessary to prevent any law enforcement or intelligence agency from crossing the line leading to potential civil rights abuses.[22] As Posner further notes, public safety and personal liberty are both constitutional values.

The challenge is to devise a system that balances law enforcement and intelligence equities, allows for information sharing, and ensures effective oversight and accountability of intelligence activities. The Geneva Centre for the Democratic Control of Armed Forces (DCAF) offers some benchmarks:

- Domestic intelligence and collection are subject to national laws.
- The separation of foreign versus domestic intelligence requires an effective coordination of collection.
- Coordination is performed by an executive branch entity.
- Joint assessments are ideally undertaken by an independent body.
- Executive, legislative, and judicial branches exercise oversight.[23]

Examining the United Kingdom's Military Intelligence 5 (MI5), the Australian Security Intelligence Organisation (ASIO), and the Indian Intelligence Bureau (IB) in terms of these benchmarks can offer ideas and insight into implementation challenges for improving homeland security intelligence in the United States. Each of the countries is similar in that they possess democratic institutions. Australia and India are more similar to the United States in that both possess a federalist type structure with the sharing of power between the federal government and state or provincial institutions. This distinction is considerably less in the United Kingdom. Additionally, India – the world's largest democracy – can be compared more readily with the United States in terms of the scope of domestic intelligence challenges. Other specific intelligence similarities and challenges include:

- The refocus of the British, Australian, and Indian intelligence on transnational terrorism and internal security issues since 9/11.

- The reorganization of the British, Australian, and Indian intelligence communities through creation of special task forces and assessment bodies focused on terrorism.
- The passage of strong anti-terror legislation and the subsequent debate over internal security and civil liberties.

There are, however, significant differences. The United Kingdom, Australia, and India possess parliamentary systems where the power of the executive is divided between the head of state and head of government. The head of government, in this case the Prime Minister, is also reliant on the support of the legislative branch or parliament. This support is expressed through a vote of confidence or no confidence. The distinction and separation between the executive and legislative branches of government is much clearer in the United States. Other differences also include the wide differences in language and culture within India versus the United States, the United Kingdom, and Australia. The ethnic differences in India have resulted in significant and recurring sectarian violence since its independence in 1947. The United Kingdom has also faced a similar issue with regard to the Irish Republican Army (IRA). Simply put, a relationship exists between countries with significant internal stability problems and the nature of the oversight mechanisms they possess. Specific differences include:

- The United Kingdom is much smaller geographically than the United States. Additionally, the United Kingdom and Australia are island nations with lesser border control and security issues as compared to the scale and scope of the United States or India.
- Indian geography – its scale and proximity to terrorist safe havens in Afghanistan, Iran, Pakistan, and the Kashmir – coupled with its much larger population and significant Muslim minority leads to greater internal security issues beyond the scale of the United Kingdom, Australia, and the United States.

Considering the similarities and differences, there is value in assessing the effectiveness of the United Kingdom's MI5, Australia's ASIO, and India's IB. The applicability of their practices will be assessed by using the DCAF's benchmarks and utilizing the following criteria:

- *Feasible*: Task can be accomplished with forces and resources.
- *Suitable*: Will mission be accomplished if tasks are carried out successfully?
- *Acceptable*: Results are politically supportable.[24]

THE UNITED KINGDOM'S SECURITY SERVICE BRANCH – MILITARY INTELLIGENCE 5 (MI5)

> "*We're always trying to improve our intelligence gathering but these groups operate in an immensely secretive way, it is very, very difficult often to track down exactly what they're doing . . .*"[25]
>
> - Tony Blair, Prime Minister of the United Kingdom

Organization. The MI5, also known as the Security Service, is the United Kingdom's domestic intelligence agency. It is responsible for responding to a wide range of security threats that include terrorism, counterintelligence, weapons of mass destruction, and organized crimes. MI5 falls under the Home Ministry, which has no precise U.S. equivalent.[26] The Security Service is one of three tier-one intelligence organizations. The Secret Intelligence Service, or MI6, focuses on foreign intelligence and the Government Communications Headquarters (GCHQ) is responsible for communications intercept and code breaking efforts.[27]

MI5 is chartered to conduct domestic surveillance operations against a wide variety of targets, but it does not possess independent arrest powers.[28] The philosophy behind this organizational relationship is to force MI5 to work hand-in-hand the various fifty-six police forces in the United Kingdom, particularly the Metropolitan and provincial Special Branches (SB).[29] As Peter Chalk states, "The Special Branch structure is the primary instrument through which intelligence is translated into operational activity and prosecutions."[30]

Despite the terrorist attacks in London (2005), the MI5 can point to credible successes. The former Director of MI5, Dame Eliza Manningham-Buller has stated that MI5 is tracking approximately 200 radical groups and over 1,600 individuals who are actively supporting or linked to terrorist activities focused on the United Kingdom – whether domestically or in foreign areas.[31] Given MI5's size, the scope of these numbers would suggest a high degree of coordination, precision, and fidelity between Britain's foreign intelligence community, its assessment bodies, and law enforcement entities.[32]

Strategic Outlook. The United Kingdom has a history of combating terrorists, particularly in its long struggle against the IRA. As a result, MI5 has an established tradition of conducting domestic intelligence operations to include electronic surveillance, recruitment, and infiltration of terrorist groups. It also has a well established working relationship with law enforcement.

The events of 9/11 fundamentally shifted the focus of the United Kingdom's intelligence apparatus. Islamic terrorism is now identified as the number one threat.[33] MI5's intelligence functions are part of a greater government counter-terrorism strategy known as CONTEST. The overarching aim of this strategy is to reduce the risk of terrorism through pursuit of four strategic approaches or lines of operation: *prevent*, *pursue*, *protect*, and *prepare*.[34] Intelligence gathering and disrupting terrorist activities are identified as two integral components under pursuit activities. MI5 performs a unique service to support these two lines of operation.[35]

Information Sharing. MI5 serves as an assessment agency as well as a collection entity. Its analysis directly supports the United Kingdom's Joint Intelligence Committee (JIC), which serves as the government's focal point for intelligence prioritization and assessment.[36] The JIC also provides regular assessments to ministers and other senior officials.[37] The establishment of the Joint Terrorism Analysis Centre (JTAC) in June 2003 (under the supervision of MI5) brings analysts from the respective intelligence agencies under one umbrella to facilitate the sharing of intelligence and breaking down of cross-agency barriers.[38] Underneath the JTAC structure, the various Special Branches have pooled their resources to develop Regional Intelligence Cells that share responsibilities and support further information sharing.[39]

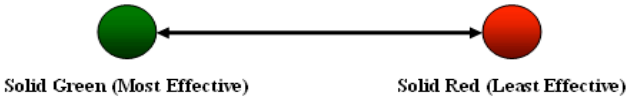
Although the United Kingdom has a highly evolved intelligence structure with a long tradition of conducting domestic intelligence, there have been several instances of information-sharing shortfalls. MI5 has been criticized for not providing warning of the Bali attacks in October 2002, the Mombasa attack in November 2002, and failing to pass specific intelligence regarding the shoe bomber, Richard Reid.[40]

The development of a strategic intelligence architecture and information sharing policies is a relevant issue for the United States. Information sharing remains a problematic issue despite the United Kingdom's well established intelligence mechanisms, clearly defined missions and roles, and assessment organs. An examination of the U.S. intelligence architecture and information sharing practices – a key 9/11 shortfall – is critical and uniquely relevant particularly given the numerous changes, reorganizations, and reforms within the U.S. intelligence community. An assessment of these changes is necessary particularly as the events of 9/11 move further into the past.

Oversight. The authority of Britain's Cabinet structure from a majority in the House of Commons affords the Prime Minister greater latitude on national security and intelligence matters.[41] Although the *Security Service Act of 1989* codified MI5's rules, missions, and functions, the intelligence and security services were largely exempt from the scrutiny of Parliament and the public until the passing of the *Intelligence Services Act of 1994*.[42] As a result of this legislation, Parliament's Intelligence and Security Committee (ISC) now reviews the budget, administration, and policy of all three intelligence agencies.[43] Its legislative oversight function, however, is much more limited that the U.S. congressional committee system.[44]

Executive oversight is also exercised by the ISC, which consists of nine members of parliament from various political parties. The ISC reports directly to the Prime Minister and is charged with producing an annual report on intelligence activities.[45] This committee operates within Britain's "ring of secrecy," which is bounded by the *Official Secrets Act*.[46] The *Official Secrets Act* allows the British government to exercise, in effect, prior restraint with respect to any disclosure of information that can be deemed harmful to the national interest.[47] Although the ISC is chartered with exercising oversight, its members are appointed by and answer directly to the Prime Minister – creating the potential for a conflict of interest. Additionally, despite the oversight mechanisms, MI5 continues to remain essentially a self-tasking organization requiring no separate approval before initiating a new operation.[48] There have also been instances of politicization, particularly during the 1980s when MI5 conducted counter-subversive operations against leftwing politicians and organizations who Prime Minister Margaret Thatcher termed, "the Enemy Within."[49]

DCAF BENCHMARKS	U.K.	Australia	India	U.S
DOMESTIC INTELLIGENCE SUBJECT TO LAWS				
COORDINATION OF DOMESTIC & FOREIGN INTELLIGENCE				
EXECUTIVE BRANCH COORDINATING				
INDEPENDENT BODY CONDUCTING ASSESSMENTS				
OVERSIGHT MECHANISMS				



Solid Green (Most Effective) Solid Red (Least Effective)

Figure 1. DCAF Benchmarks versus the U.K.

Conclusion. MI5's strengths lie in its ability to operate under a well defined executive structure that utilizes an independent intelligence assessment umbrella and operates under a well understood set of laws. The organization also has a long history of performing its internal security and domestic intelligence functions. The United Kingdom also possesses several highly evolved mechanisms to coordinate the sharing of intelligence. Despite this structure, there have been several instances where MI5 did not share its intelligence. Effective intelligence sharing remains an issue. Although there are existing oversight mechanisms, the structure of the United Kingdom's oversight organs also inhibits significant legislative oversight of the intelligence process. Utilizing the DCAF benchmarks listed in Figure 1, the United Kingdom's strengths lie in its strong executive coordination and independent assessment process. Its domestic intelligence agency also operates under a well defined set of national laws, although the effectiveness of information sharing remains an issue. Lastly, given the United Kingdom's oversight structure and MI5's past abuses, the oversight and accountability mechanisms that balance civil liberties versus public safety remain a potential area of concern. An assessment of information-sharing practices and oversight procedures – given the numerous changes within the U.S. intelligence community and the recent FBI controversy on the handling and accountability of National Security Letters – is of particular relevance for the United States.

THE AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION (ASIO)

"*In the difficult fight against the new menace of international terrorism, there is nothing more crucial than timely and accurate intelligence.*"[50]
John Howard, Australian Prime Minister

Organization: The Australian Security Intelligence Organisation (ASIO) serves as Australia's domestic intelligence organization. Similar to MI5, it is chartered to address a wide variety of threats.[51] ASIO works closely with the Australian Protective Service

(APS), with both agencies falling under Australia's Attorney General.[52] ASIO is also one of three tier-one intelligence organizations. The Australian Secret Intelligence Service (ASIS) functions as the foreign intelligence entity while the Defence Signals Directorate (DSD) is focused on signals intelligence.[53]

Heavily influenced by the British philosophy of separating domestic intelligence and law enforcement powers, ASIO does not have independent arrest powers.[54] As such, ASIO must work closely with police entities particularly the APS – roughly equivalent to the FBI or the Royal Canadian Mountain Police (RCMP). The primary venue for APS-ASIO interaction is through the National Threat Assessment Centre, which serves as the focal point for collaboration with federal organization and state police forces.[55]

Strategic Outlook. Australia does not have a long history of combating terrorists. It has not been plagued by an internal threat (like the United Kingdom and the IRA) or India's numerous internal security issues due to its linguistic and ethnic differences. Additionally, Australia has been largely isolated by the nature of its geography. As a whole, Australia has typically viewed its strategic threats in a foreign context and has prized the value of international cooperation with its allies to deal with its security issues.

Despite its lack of internal threats, the Australian government has taken a serious and very thorough approach to internal security. It went through significant security preparations for the Sydney 2000 Olympic Games, which also highlighted the value of international cooperation.[56] The Australian government now recognizes Islamic terrorism as its highest threat priority and has committed significant resources to counterterrorism as a result of the 9/11 attacks and al Qaeda statements that identify Australia as a target.[57] ASIO's intelligence function operates as part of the government's four pronged counterterrorism approach: *prevention*, *preparedness*, *response*, and *recovery*. Improving intelligence capacity, increasing the effectiveness of information sharing, seeking better detection capabilities, and improving law enforcement coordination are the overarching themes under prevention and preparedness.[58]

Despite the lack of a historical internal security threat or Australia's priority as a target for a terrorist attack, the ASIO can point to some success in categorizing and tracking domestic terrorist threats. Similar to the MI5, ASIO also has the reputation for thoroughness and developing precise intelligence. On November 18, 2005, Australian authorities foiled the activities of two terrorist cells. ASIO and Australian law enforcement agencies were able to prevent an attack possibly aimed at critical infrastructure as a result of an eighteen-month long investigation into individuals with possible linkages to al Qaeda and radical Kashmiri groups.[59]

Information Sharing. Like MI5, ASIO also serves as an analytic assessment agency. The Office of National Assessment (ONA) serves as Australia's premier strategic assessment organization. ONA, ASIO, ASIS, and DSD also enjoy close access to the Prime Minister's Office.[60] The National Intelligence Group (NIG), which resides under ASIO, collates intelligence from multiple sources and disseminates products to governmental and law enforcement officials through Joint Intelligence Groups.[61] Executive coordination of domestic intelligence and other matters is accomplished through the National Security Committee of Cabinet (NSC) and the Secretaries' Committee on National Security (SCoNS). The NSC consists of senior policy makers

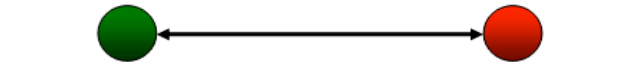
while the SCoNS consists of department secretaries who, like those in the United Kingdom, are professional bureaucrats.[62]

Although Australia's intelligence system is modeled on the United Kingdom's, with domestic intelligence having to work closely with law enforcement entities, there have also been corresponding shortfalls in information sharing. ASIO's performance was also criticized for disregarding threat assessments from regional analysts regarding the Bali attack in 2002 – an area directly under ASIO's concern.[63] Like the United Kingdom, Australia has a highly defined intelligence community; however, its track record on information sharing is an issue. Despite Australian and British similarities and the ability of their domestic intelligence agencies to possibly develop greater precision in categorizing the domestic threat, their identified information sharing problems remain a relevant issue for the United States.

Oversight. ASIO's statutory responsibilities are outlined in the *ASIO Act of 1979*. Although Australia is similar to the United Kingdom, there is a greater distinction between executive and legislative oversight roles. The *Intelligence Services Act of 2001* expanded the role of the Parliamentary Joint Committee on Intelligence and Security in overseeing Australia's intelligence apparatus.[64] The committee can initiate investigations or respond to requests from the Attorney General requests.[65] Australia's executive oversight is also more robust. The Inspector General of Intelligence and Security (IGIS) is an independent officer appointed by the Governor-General and located within the Prime Minister's office. This unique arrangement allows the IGIS to assist the government and parliament in oversight matters, but allows the office to act independently. The IGIS also enjoys total access to all intelligence and possesses the power of independent inquiry.[66] This oversight also includes access to case files, warrant powers, and financial records.

Although not a method of oversight, the Australian government also has an aggressive public outreach program. The federal government has established National Security Public Information Guidelines for all agencies engaged in national security issues to promote the public's understanding of the missions and threat. A National Security Public Information Campaign also seeks to encourage public vigilance. Security information is pushed via a variety of media means to inform the Australian public of the government's efforts against terrorism and to create a safer environment.[67] These efforts directly support ASIO's efforts in engaging communities to derive community-based information conduits to support its assessments. This is in stark contrast to MI5's historical outlook regarding public engagement, which took the major step of instituting a public website only after 9/11.[68] Despite these strong oversight mechanisms, ASIO has also been criticized for heavy-handed and intrusive tactics in the past against leftwing groups.[69]

DCAF BENCHMARKS	U.K.	Australia	India	U.S
DOMESTIC INTELLIGENCE SUBJECT TO LAWS				
COORDINATION OF DOMESTIC & FOREIGN INTELLIGENCE				
EXECUTIVE BRANCH COORDINATING				
INDEPENDENT BODY CONDUCTING ASSESSMENTS				
OVERSIGHT MECHANISMS				



Solid Green (Most Effective) Solid Red (Least Effective)

Figure 2. DCAF Benchmarks versus the U.K.-Australia

CONCLUSION. ASIO's strength, like MI5, lies in its ability to operate under a well defined structure and an independent assessment umbrella. ASIO also has a long history in internal security and domestic intelligence. Despite possessing a highly evolved information sharing structure, there have also been corresponding shortfalls in ASIO's information sharing performance. Lastly, Australia has robust executive and legislative oversight mechanisms, which although not possessing a perfect track record, are effective in overseeing the country's intelligence process. An examination of Australian oversight mechanisms and public outreach programs may offer some areas for improvement in the United States. When compared against the DCAF benchmarks in Figure 2, Australia's top strengths lie in its strong laws governing domestic intelligence, the ability of the executive body to coordinate intelligence, and its independent assessment capability. Similar to the United Kingdom, it also has faced some information sharing shortfalls and although it possesses a better defined executive and legislative oversight process, there have been instances of past abuse.

THE INDIAN INTELLIGENCE BUREAU (IB)

> "*We are fully on board as far as the global war against terror is concerned. We will cooperate with everybody, bilaterally, regionally, at the global level, in the fight against terror.*"[70]
> Manmoham Singh, Prime Minister of India

Organization. The Intelligence Bureau (IB) functions as India's internal security agency.[71] One of the longest functioning intelligence agencies, its roots can be traced back to the Imperial Intelligence Bureau, which served British interests in India.[72] It is chartered with a wide range of responsibilities spanning from combating terrorists and the separatist efforts of *Naxalists* (Indian Maoists) to critical infrastructure protection – particularly aviation security.[73] The IB falls under India's Ministry of Home Affairs although the Director of the IB can report to the Prime Minister on intelligence issues.[74] Unlike the United Kingdom and Australia, which possess separate foreign

espionage and signals intelligence organizations, India's Research and Analysis Wing (RAW) oversees all of India's foreign intelligence.[75] Similar to MI5 and ASIO, the IB does not have independent arrest powers and must rely on federal and state law enforcement elements.

India has been hard pressed to reform its intelligence apparatus. Following the eleven-week skirmish in 1999 with Pakistan, the Group of Ministers (GoM) initiated a major study of India's security and intelligence. This study, headed by former RAW director, Girish Saxena, submitted numerous recommendations to streamline the intelligence process.[76] The Saxena Committee performed the first major review of Indian national security and intelligence since its independence in 1947.[77] For the IB, these initiatives included the development of an independent signals intelligence capability, an expansion of the IB's field presence by bolstering its Subsidiary Intelligence Bureaus (SIB) at the state level, implementation of Inter-State Intelligence Support Teams, development of Joint Task Forces for Intelligence (JTFIs), and a Multi Agency Centre (MAC) to electronically collate and database related intelligence.[78]

Despite its promise, most of the reforms have not been implemented – largely due to bureaucratic infighting. The Ministry of Home Affairs and the Ministry of Finance have disapproved the key elements recommended by the committee.[79] The development of the IB's signals intelligence capability has been stalled. The Finance Ministry has disapproved the IB's request for computer trained personnel to develop and maintain the MAC. Funding for the JTFIs and associated training has also been cut. This bureaucratic confrontation is attributable to the long standing infighting between the Indian Administrative Service officers who dominate the Home ministry and the Indian Police Service officers who constitute the majority of the IB.[80] The inability the Indian government to institute meaningful intelligence reforms, establish clear organizational mission roles and responsibilities, and manage the competitive tensions between different bureaucracies are of critical importance given the similarities of the U.S. intelligence community and its efforts to reform itself, institute organizational change, and establish a strategic approach to combating terrorism in a post 9/11 environment.

Strategic Outlook. India has faced many internal security problems since establishing its independence in 1947. Consisting of a multitude of ethnicities, languages, and particularly due to the partition of India and Pakistan, India has faced numerous acts of sectarian violence. In 1999, the hijacking of Indian Airlines flight 814 prompted calls for stronger anti-terrorism legislation. The subsequent events of 9/11 affected the Indian government's perception of the al Qaeda threat and provided an opportunity for parliamentarians to enact stronger legislation that addressed transnational terrorism and financing issues.[81] In 2002, the legislature, led by the nationalist Bharatiya Janata Party, passed *The Prevention of Terrorism Act (POTA)* – a strong anti-terror legislation similar to the United States, the United Kingdom, and Australia.[82] The legislation came under severe criticism and was later repealed in 2004 with the entrance of a new government under the opposing Congress party.[83] The July 2006 terrorist attacks in Mumbai have renewed the demands for more stringent anti-terrorism legislation.

Although the Indian government has recognized the threat posed by al Qaeda through its proximity to the Indian subcontinent, the government has been unable to articulate precisely its approach to combating terrorism. A key shortfall in the *POTA*

legislation was that it lacked any linkage to a wider counterterrorism strategy and approach. As Swati Pandey states:

> For a counterterrorism law, lawmakers should consider the state's police capabilities, the legal system, and the political leanings of its population to make sure that the law will be successful. If these means are sufficient, then the goals of the law can be reached.[84]

The absence of political buy-in, unclear linkages between the legislation's intent and the actual capabilities of security forces, and poor existing oversight mechanisms result in a mismatch between the strategic vision versus actual practice. The Indian government's approach has been erratic with limited consensus between political parties. These inconsistencies stem from India's longer-term inadequacy in managing national security. As B. Raman asserts, this is due to three factors:

> The absence of long-term thinking and planning are due to preoccupation with day-to-day crisis management and short-term compulsions, the inhibition of fresh thinking and a coordinated approach to national security issues due to the undue influence of narrow departmental mindsets, and the absence of a watchdog set-up, uninfluenced by departmental loyalties, to monitor the implementation of the national security decisions and remove bottlenecks.[85]

Given this framework and unlike MI5 and ASIO, the role of the IB is less clear. The IB clearly has many domestic intelligence functions. Conversely, unclear strategic guidance, obscured responsibilities, bureaucratic infighting, and extremely limited oversight mechanisms severely hamper its ability to execute its mission. The Indian shortfalls of translating strategic intent into coherent intelligence reform and community management is of paramount – *indeed critical* - importance for the United States as it attempts to redefine its intelligence apparatus in a post 9/11 environment.

Information Sharing. The challenges faced by the IB are also a reflection of the Indian national security apparatus. The Saxena Committee recommended the implementation of an Intelligence Coordination Group (ICG) and Technology Coordination Group (TCG) to work closely with the National Security Council Secretariat (NSCS) and the Joint Intelligence Committee (JIC).[86] These groups were intended to focus on resource allocation, annual reviews, national estimates, and executive oversight.[87]

Bureaucratic infighting has also plagued the information sharing and assessment process. The National Security Council (NSC), revived as part of the committee's recommendations, has been ineffective in orchestrating the various agencies towards a single purpose.[88] The NSC is rarely convened and does not have a dedicated staff structure to support this process.[89] Senior officials also state that there is little to no coordination between the IB, RAW, and the newly formed Defence Intelligence Agency (DIA).[90]

Although India's organizational structures are similar to the United Kingdom and Australia, they are not as developed or resourced. Bureaucratic infighting and the lack of strong executive direction have limited the IB's effectiveness. There is also an inherent instability in India's organizational approaches and processes to managing national security and intelligence functions.[91] Despite its responsibility for domestic intelligence, the IB has not been given the requisite tools to perform varied responsibilities. As Praveen Swami, an Indian journalist noted for his coverage of

Indian national security issues commented, "The head of the U.S.' Federal Bureau of Investigation can authorize the cash down purchase of millions of dollars of equipment, while the Director of India's Intelligence Bureau cannot authorize the purchase of a new desktop computer for his secretary."[92]

Oversight. The Saxena Committee also attempted to address oversight issues by defining India's different intelligence agency's missions and roles and to ensure executive oversight via the NSCS.[93] The inability to implement these reforms, particularly at the executive and assessment level, has resulted in little progress. Additionally, abuse of the *Official Secrets Act of 1923* prohibits national security issues from coming into the forefront of public debate.[94] As Sarath Ramkumar notes, "Top-level political appointees quickly become vigilant in seeking to preserve three main bureaucratic prerogatives of secrecy: control over preservation, control over custody and control over access."[95]

In the absence of a wider public debate, India's parliamentary members rarely discuss or understand the wider implications of India's intelligence issues.[96] In fact, the IB and the RAW are not formally accountable to the parliament.[97] The lack of an effective oversight structure leads to India's legislature being removed from the process. The Standing Committee on Home Affairs has received briefings on the IB's activities, but few of its members have a background in intelligence or are sufficiently staffed to exercise effective oversight.[98] Ramkumar offers the following insightful assessment of India's intelligence community:

> Intelligence agencies are not islands that exist outside executive control. The usefulness and the quality of intelligence is only as good as the government of the day requires. Any serious reforms in the field of intelligence need an understanding of the precise role of intelligence agencies in serving the nation's national security interest.[99]

The lack of executive and legislative oversight mechanisms has resulted in the politicization of the IB. Most of the bureau's focus has been on political surveillance and election-related information gathering in support of the ruling party.[100] As one member of the National Security Advisory Board commented recently, "How can we expect the IB to function if a large part of its resources is directed at serving the ruling political party of the day?"[101]

Although the United Kingdom and Australia have suffered from oversight shortfalls, the Indian shortcomings in this area have hampered greater intelligence reforms. Understanding the linkage between implementing reform and oversight, given the challenge faced by the Indian government, is of unique importance for the United States. Improving the effectiveness of intelligence oversight – an identified 9/11 recommendation – serves to link the intent and vision of national strategy to the implementation of intelligence reforms.[102]

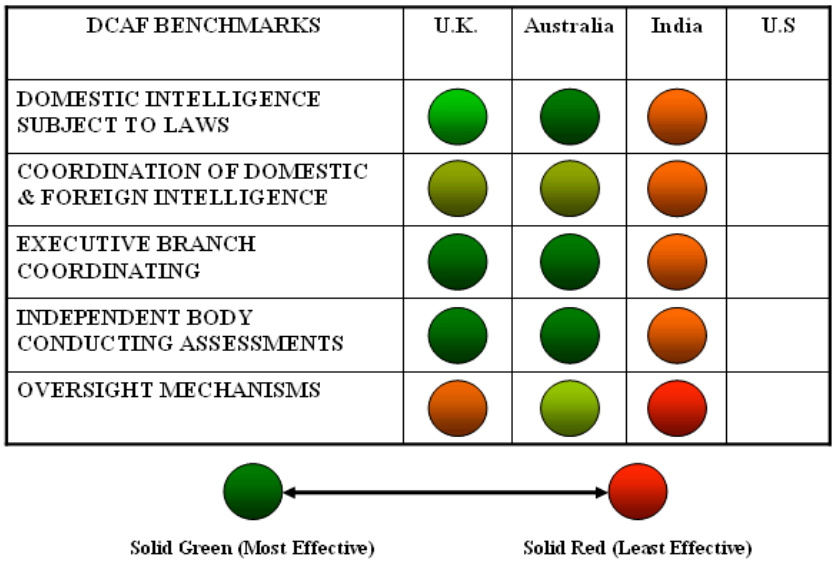


Figure 3. DCAF Benchmarks versus the U.K.-Australia-India

Conclusion. The IB has not been given the necessary tools and resources to fulfill its mission. Although the IB has a long history of performing its internal security function, the majority of its focus has been on political surveillance. Despite sound recommendations and higher-level organizational initiatives, bureaucratic infighting and petty competition have inhibited translating these initiatives into meaningful activities. Lastly, despite possessing definitive intelligence organizations and mandated assessment entities, the lack of strong executive direction and bipartisanship, weak legislative oversight, organizational instability, and ineffective resourcing have resulted in a listless national security and intelligence apparatus. These limitations, when compared to the DCAF benchmarks in Figure 3, display a marginal effectiveness. India's intelligence apparatus does not operate under a well defined set of laws and coordination between intelligence agencies remains an endemic problem. Its independent assessment capability has not been properly resourced and bureaucratic infighting greatly inhibits the ability of the executive to coordinate and direct intelligence efforts. Lastly, India's almost total lack of executive and legislative oversight severely limits accountability and the ability to reform the system.

DOMESTIC INTELLIGENCE AGENCY: APPLICATION FOR THE UNITED STATES?

Proponents of a domestic intelligence agency highlight the importance of prevention, yet domestic intelligence agencies focused solely on information gathering and developing sources have not been proven to be more effective in preventing terrorist attacks. They may have a greater ability to develop better and more precise intelligence assessments on the nature of the domestic threat. The bombings in London (2005) and Mumbai (2006), however, highlight the point that not all attacks can be prevented. Additionally, the metrics for how many attacks have been prevented and where these agencies can cite unreported successes is absent due to their classified nature. By

examining the United Kingdom, Australia, and India, it is evident that the challenges of coordinating intelligence, sharing information, and implementing oversight mechanisms are problematic and relevant issues for their domestic intelligence agencies.

Organization. For the United States, intelligence coordination and assessment were highlighted as significant shortfalls after 9/11. Although the United States does not have an assessment apparatus as highly centralized and evolved as the United Kingdom or Australia, it has been recognized as a shortfall and steps have been taken to address this issue. The major change was the creation of the Department of Homeland Security with an intelligence charter. The U.S. government also adopted measures to implement intelligence coordination and improve identified shortfalls through the creation of the Director for National Intelligence (DNI), the National Counter Terrorism Center (NCTC), and revamping the FBI's intelligence capability.[103] Calls for further FBI reforms have continued. As a result of further findings, the FBI consolidated many of its intelligence functions under the creation of the National Security Service.[104] Despite the creation of these new agencies and initiatives, the effectiveness of these organizations to implement and institutionalize intelligence reforms, manage resources, and develop strategic assessments as envisioned in the national strategy is questionable, particularly since these initiatives have occurred within a relatively short period of nearly six years after 9/11 and given similar Indian attempts over the last decade.

Information Sharing. As with the United Kingdom, Australia, and India, information sharing is a significant issue for the United States. This is recognized as a core issue in the *National Intelligence Strategy for the United States*.[105] Further measures have been taken to address this issue through creating the NCTC, instituting the DHS, reforming the FBI's headquarters, implementing Field Intelligence Groups (FIGs), and developing state intelligence fusion centers. The domestic intelligence challenge in the United States is similar to India's in terms of organization and the scope of the problem. Despite higher level initiatives, the FBI continues to have a "law enforcement" mindset, is experiencing similar problems with implementing its information sharing technology, and is faced with coordinating with multiple state and local efforts.[106] The DHS has also been faced with similar bureaucratic hurdles. Additionally, there is no clear linkage or relationship between the NCTC and the numerous state and local fusion centers that have been created since 9/11.[107] As a result, the level of integration remains questionable. Despite the plethora of executive findings and directives, there are still significant bureaucratic hurdles and infighting to sharing information.

Oversight. Intelligence oversight remains an issue for the United States. Controversies such as the National Security Agency's (NSA) electronic surveillance and the Department of Defense's Counter Intelligence Field Activity's (CIFA) monitoring of U.S. persons, the intelligence activities in Guantánamo, and the handling of National Security Letters remain at the forefront of the political debate. Intelligence initiatives have been undertaken since 9/11, but most of these efforts – particularly with regard to domestic intelligence – have received significant criticism due to ineffective implementation efforts and a lack of bipartisan buy-in. While oversight issues are also challenges for MI5, ASIO, and the IB, Australia seems to have a highly developed,

resourced, and aggressive executive and legislative oversight component. A closer examination of Australia's oversight practices and mechanisms could yield practical lessons for the United States. Additionally, the United States needs to streamline and improve its legislative oversight process – a key recommendation of the 9/11 Commission – to ensure proper safeguards for civil liberties and accountability of intelligence operations.[108] Progress in this area has been tepid.

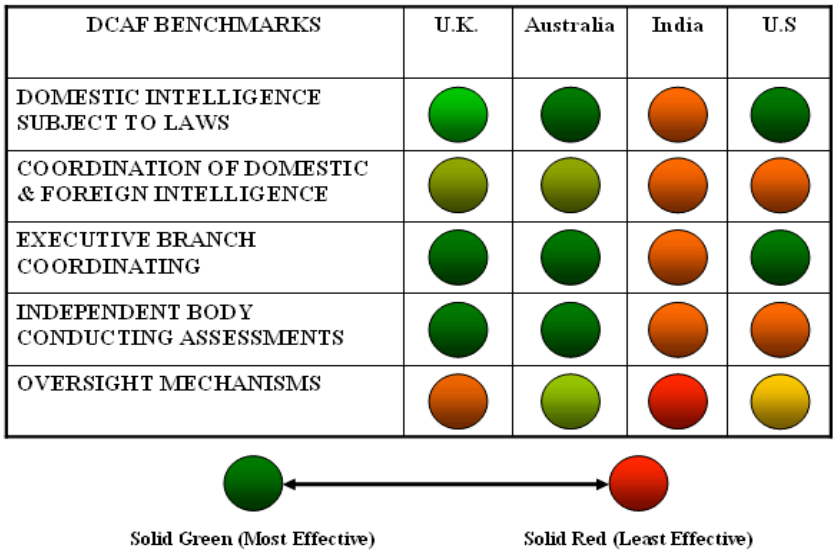


Figure 4. DCAF Benchmarks versus U.K.-Australia-India-U.S.

Conclusion. When compared to the DCAF benchmarks in Figure 4, the United States possesses a well defined set of laws operating under a strong executive mechanism. These strengths, however, are offset by a weaker executive and legislative oversight process. Although U.S. oversight mechanisms limit the statutory ability of the FBI and other agencies to conduct domestic intelligence, there are still oversight shortfalls in terms of staffing, resources, and legislative access. As seen in the Indian case, limited oversight can also lead to poor implementation of intelligence initiatives. Although there have been numerous fact-finding commissions, such as the 9/11, the *Commission on Intelligence Capabilities of the United States regarding Weapons of Mass Destruction*, and the numerous panels prior to 9/11, there has not been a strategic and bipartisan approach to overseeing and tracking the implementation and effectiveness of these reforms. Lastly, although steps have been taken to institutionalize the NCTC's independent assessment capability and fuse domestic and foreign intelligence, it is uncertain whether these steps are translating into positive action, whether they are truly combining with the efforts of the DHS or regional, state, or large metropolitan fusion centers, or whether an additional layer of bureaucracy has been added to an already heavily bureaucratized intelligence apparatus.

SUMMARY

Although domestic intelligence agencies possess several shortfalls in not being able to prevent terrorist attacks and have corresponding information-sharing shortfalls and oversight issues, these shortfalls do not address the entire scope of the problem. While domestic intelligence agencies may not be able to prevent all terrorist attacks, are they more successful in preventing most attacks? Do effective domestic intelligence agencies, solely focused on intelligence gathering and unencumbered by law enforcement responsibilities, possess a better ability to focus and develop precise intelligence? Without access to classified sources or performance measures, most literature would suggest that domestic intelligence agencies are more effective in developing intelligence through the penetration of terrorist cells and collation of other intelligence data.[109]

Additionally, the combination of law enforcement and intelligence functions under the FBI and the Attorney General, acting as the federal government's chief legal officer, has also led to civil rights abuses. Opponents to the creation of a domestic intelligence agency fail to recognize that the argument for separating domestic intelligence from law enforcement functions was precisely the reason for limiting the West German government's ability to exercise arbitrary power when it was reconstituted as a nation in the 1950s.[110] In other words, the German domestic intelligence apparatus was consciously separated from law enforcement responsibilities to prevent an abuse of power. Balancing civil rights and public safety remains a problematic issue for democracies whether they possess a domestic intelligence agency or not.

Despite the arguments posed by the advocates for and opponents to having a domestic intelligence agency for the United States, an examination of MI5, ASIO, and the IB have shown that domestic intelligence agencies are not necessarily the solution to addressing the domestic intelligence gap. They may possess a greater ability to better categorize threats and operate unencumbered by complicated and competing mission roles within one agency. In terms of the feasibility, suitability, and acceptability of implementing this organizational construct for the United States, it is *feasible* to develop a U.S. domestic intelligence agency if the resources and executive direction are applied to instituting this capability. The critical *feasibility* issue, however, is whether the United States can translate strategic guidance and direction into meaningful change, reform, and capability that mitigates the domestic intelligence gap – whether under a domestic intelligence agency or some other organizational construct. This is the clear lesson from India's attempt to reform the IB and institute larger intelligence reforms.

Suitability (whether the mission will be accomplished if the tasks are carried out successfully) is also contingent on the ability to translate strategic intent into meaningful change. The 9/11 Commission did not see a need to create a domestic intelligence agency *unless their other recommendations were not adopted* – to create an effective NCTC and Director of National Intelligence (DNI).[111] The effectiveness of the DNI to implement reform was questionable when 96 percent of the FBI's intelligence function fell *outside* of the DNI's purview.[112] Continued FBI reform attempts, as evidenced by reorganization efforts in 1998, 1999, 2000, and 2001, are indicative of organizational instability or resistance to change.[113] Organizational instability and resistance to change can also be applied to NSA. Additionally, the

obstacles to creating a unified DHS are another indication of bureaucratic intransigence. The implementation of a strategic vision into reality is clearly a challenge that India has had to face. These shortfalls and others would indicate that current tasks and reforms are not being effectively implemented.

Like the United States, the United Kingdom, Australia, and India have been unable to prevent terrorist attacks. In the absence of definitively demonstrating that domestic intelligence agencies are better positioned to prevent most attacks, the single largest obstacle to implementing this organizational construct in the United States is cultural. Given the history and structure of the United States, it is probably still not *acceptable* to have a domestic intelligence agency. Although the political supportability was stronger after 9/11, most Americans do not like to feel that they are being spied upon by their government or neighbors.[114] Additionally, as Kate Martin points out, "Nothing in the pre-September 11 law prevented the CIA from informing the FBI that the suspected terrorists had entered the United States, and nothing would have prevented the FBI from pursuing them."[115] The issue lies in the practical interpretation of these regulations. It was the inability to effectively put these regulations into practice that led to information-sharing shortfalls prior to 9/11. It is also the inability to effectively implement the post 9/11 regulations and intelligence initiatives through a bipartisan approach – such as the NSA monitoring program – that creates continued foreign-domestic information sharing gaps.

The central issue is not whether to have a combined law enforcement and intelligence organization versus a sole domestic intelligence agency. The issue is effective *organizational reform*, *information sharing*, and *oversight*.[116] Effective organizational change, information sharing, and oversight are not necessarily achieved through high-level organizational repositioning, implementing common information data systems, or passing new regulations for managing intelligence operations and reform. The absence of a significant terrorist attack in the United States since 9/11 is also not a good indicator that the intelligence apparatus is operating more efficiently. The creation of additional bureaucracies, an increased centralization of intelligence functions that inhibits the analysis of opposing alternatives, and the inability of the U.S. Congress to reform its oversight process may have actually led to greater drawbacks rather than progress. Although the United States has developed strategies and applied significant resources to address its weaker areas – such as the creation of the DNI to oversee the intelligence community, the NCTC to integrate domestic-foreign intelligence and develop assessments, and the professionalization of the DHS and the FBI's intelligence functions – there remains a level of uncertainty whether these initiatives have resulted in greater progress and meaningful transformation. This uncertainty continues to place the United States at risk. To address these information sharing and oversight uncertainties, the following actions are recommended:

- Assess the ability of the DNI to exercise leadership and management over the intelligence community in terms of controlling resources, implementing cross-organizational information sharing initiatives, and effecting reform consistent with the *National Intelligence Strategy for the United States*. This is a clear lesson learned from similar Indian attempts to reform its intelligence community since the 1999 GoM findings.

- Capitalizing on the British and Australian strengths in developing strategic assessments and categorizing domestic threats, conduct an end-to-end organizational review of NCTC to analyze its performance compared to its stated mission, particularly its ability to support its domestic intelligence assessment within a *national* and not strictly federal context.
- Given the identified information-sharing shortfalls with countries possessing domestic intelligence agencies, conduct a review of information sharing and knowledge management policies to assess the applicability of current policies versus actual practice, most notably providing warning and the sharing of raw and unevaluated intelligence between organizations.[117]
- Review the FBI's and DHS's intelligence reform initiatives in terms of professionalization, information sharing, strategic focus, and resource allocation to determine if there is a continued law enforcement versus intelligence mindset, as evidenced by Indian bureaucratic infighting.
- Drawing from Australian strengths, reevaluate executive and congressional oversight mechanisms and reforms to identify duplicative functions, staffing, resources, and the ability to link strategic intent to implementation of intelligence reforms.

Merely implementing a U.S. domestic intelligence agency will not prevent further terrorist attacks. Although the domestic intelligence agencies of the United Kingdom, Australia, and to a lesser extent, India, have had their successes, they have also suffered the same shortcomings of the United States in terms of information sharing and oversight. Additionally, there have been numerous organizational changes and attempts at reform since 9/11. Only an in-depth appraisal of the DNI and NCTC's performance, the ability of intelligence and law enforcement organizations to share information, the FBI's progress at reforming itself, the implementation of the DHS as an organization with a domestic intelligence function, and the ability to provide effective oversight will determine whether the intelligence shortfalls identified in the congressional inquiry into the attacks on 9/11 have been addressed.[118]

LCDR James Burch has been in the Navy for eighteen years as a Naval Cryptologist and is currently assigned to U.S. Northern Command as the Deputy Chief of Collection Management within the Intelligence Directorate. He was most recently assigned to CRUISER DESTROYER GROUP TWO as part of the GEORGE WASHINGTON Battle Group from 2001-2003, which deployed off the coast of New York City after 9/11 and later participated in Operation Enduring Freedom. After his assignment, he attended the U.S. Army's Command and General Staff College (CGSC) in Leavenworth, Kansas. LCDR Burch's educational background consists of a B.S. in Marine Transportation from the U.S. Merchant Marine Academy and an M.A. in Military History from CGSC. He also attended the Naval Command & Staff College via the Navy's seminar program and the Joint Forces Staff College.

1 U.S. Congress, House, Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd Session,December 2002, S. Rept. No. 107-531, H. Rept. No. 107-792, 244. http://www.fas.org/irp/congress/2002_rpt/911rept.pdf.

2 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2003), 353. The inability to manage and fuse foreign and domestic intelligence information was identified as a key shortfall.

3 Gregory F. Treverton, "Intelligence, Law Enforcement, and Homeland Security," *The Century Foundation* (January 8, 2002): 1. http://www.tcf.org/Publications/HomelandSecurity/treverton-intelligence.pdf.

4 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 172. The estimate for al Qaeda's monetary cost to plan and execute the 9/11 attacks ranges from $400,000 to $500,000 dollars.

5 U.S. Congress, Senate, *Homeland Security Act of 2002*, Public Law 107-296, sec. 101 (2002), 13; http://fl1.findlaw.com/ news.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf. Section 101 established the Department of Homeland Security and reorganized several preexisting government agencies under the department.

6 Permanent Select Committee on Intelligence, *Report of the Joint Inquiry*, 245.

7 Paul R. Pillar, "Intelligence," in *Attacking Terrorism: Elements of a Grand Strategy* (Washington, DC: Georgetown University Press, 2004), 134.

8 Mark W. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed (Washington, DC: CQ Press, 2006), 234.

9 Harry Howe Ransom, "The Politicization of Intelligence," in *Strategic Intelligence: Windows Into A Secret World*, ed. Loch K. Johnson and James J. Wirtz (Los Angeles, CA: Roxbury Publishing Company, 2004), 175.

10 Harvey Rishikof, "The Role of the Federal Bureau of Investigation in National Security," in *Intelligence and National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George and Robert D. Kline (New York: Rowan & Littlefield Publishers, Inc., 2006), 126; The Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (October 2002), 21. http://www.markle.org/downloadable_assets/nstf_full.pdf.

11 Michael Massing, "A War on Terrorism is Futile," in *Are Efforts to Reduce Terrorism Successful?*, ed. Lauri S. Friedman (New Haven, CT: Greenhaven Press, 2005), 25.

12Permanent Select Commmittee on Intelligence, *Report of the Joint Inquiry*, 245.

13 Larry M. Wortzel, "Americans Do Not Need a New Domestic Spy Agency to Improve Intelligence and Homeland Security," *The Heritage Foundation*, no. 848 (January 10, 2003): 2. http://www.heritage.org/Research/ HomelandDefense/loader.cfm?url=/ commonspot/security/getfile.cfm&PageID=34700.

14 Eric R. Taylor, "The Department of Homeland Security May Make Americans Less Safe," in *Homeland Security*, ed. James D. Torr (New Haven, CT: Greenhaven Press, 2004), 64.

15 Ibid., 61.

16 Frederic R. Manget, "Another System of Oversight: Intelligence and the Rise of Judicial Intervention," in *Strategic Intelligence: Windows Into A Secret World*, ed. Loch K. Johnson and James J. Wirtz (Los Angeles, CA: Roxbury Publishing Company, 2004), 408.

17 B. Raman, *Intelligence: Past, Present, and Future* (New Delhi, India: Lancer Publishers & Distributors, 2002), 6.

18 Manget, "Another System of Oversight: Intelligence and the Rise of Judicial Intervention," 408; Rishikof, "The Role of the Federal Bureau of Investigation in National Security," 126.

19 Ransom, "The Politicization of Intelligence," 171.

20 Ibid., 175.

21 Benjamin Netanyahu, *Fighting Terrorism: How Democracies Can Defeat the International Terrorist Network* (New York: Farrar, Straus and Giroux, 1995), 30.

22 Richard A. Posner, *Remaking Domestic Intelligence* (Palo Alto, CA: Hoover Institution Press, 2005), 73.

23 Geneva Centre for Democratic Control of Armed Forces, "Intelligence Services and Democracy," no. 13, Geneva Centre for the Democratic Control of Armed Forces (DCAF) (April 2002):3-13, http://www.dcaf.ch/_docs/WP13.pdf (accessed on December 31, 2006).

24 Department of Defense, *Joint Staff Officer's Guide* (Washington, DC: GPO, 2000), 4-87, G-75.

25 Tony Blair, "BBC Breakfast with Frost Interview," interview by Sir David Frost, *British Broadcasting Corporation (BBC)* (30 September 2001); http://news.bbc.co.uk/1/hi/programmes/breakfast_with_frost/1571541.stm.

26 Lowenthal, *Intelligence: From Secrets to Policy*, 291.

27 Frank Gregory, "Intelligence led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005," *Real Instituto Elcano de Estudios Internacionales y Estratégicos,* no. 94 (7 December 2005), 3; http://www.realinstitutoelcano.org/analisis/781/Gregory781-v.pdf.

28 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, Hearing Before a Subcommittee of the Committee on Appropriations, 109th Congress, 2nd Session (September 14, 2006), 23; http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:30707.pdf.

29 Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI5 Model to the United States (*Washington DC: The Library of Congress, 19 May 2003), 6; http://www.fas.org/irp/crs/RL31920.pdf.

30 Peter Chalk and William Rosenau, *Confronting the Enemy Within: Security Intelligence, The Police, and Counterterrorism in Four Democracies* (Santa Monica, CA: RAND Corporation, 2004), 12. http://www.rand.org/pubs/monographs/2004/RAND_MG100.pdf.

31 Jane's Intelligence Digest, *Britain: intelligence versus terrorism* (London: Jane's Information Group, 2006), 1.

32 According to MI5, the Security Service currently employs approximately 2,800 persons. The organization as a whole has experienced targeted growth since 9/11. See MI5's website at www.mi5.gov.uk.

33 Her Majesty's Government, *Countering International Terrorism: the United Kingdom's Strategy*, CM6888 (July 2006), 16; http://www.mi5.gov.uk/files/pdf/ct_strategy.pdf.

34 Ibid., 2.

35 Ibid., 16.

36 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, 22.

37 Chalk and Rosenau, *Confronting the Enemy Within*, 10.

38 Paul Tumelty, "An In-Depth Look at the London Bombers," *Terrorism Monitor* 3, no.15 (July 28, 2005): 4; http://jamestown.org/terrorism/ news/uploads/ter_003_015.pdf.

39 Gregory, "Intelligence led Counter-terrorism," 3.

40 Jim Dempsey, "Domestic Intelligence Agencies: The Mixed Record of the UK's MI5," *Center for Democracy and Technology* (27 January 2003), 2; http://www.cdt.org/security/usapatriot/030127mi5.pdf.

41 Masse, *Domestic Intelligence in the United Kingdom*, 6.

42 Chalk and Rosenau, *Confronting the Enemy Within*, 31; Gregory, "Intelligence led Counter-terrorism," 3.

43 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, 28.

44 Lowenthal, *Intelligence: From Secrets to Policy*, 292-293.

45 Chalk and Rosenau, *Confronting the Enemy Within*, 14-15.

46 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, 28.

47 Masse, *Domestic Intelligence in the United Kingdom*, 9. The doctrine of prior restraint was deemed unconstitutional in the United States in the *New York Times v. United States (1971).*

48 Chalk and Rosenau, *Confronting the Enemy Within*, 51, 53.

49 Ibid., 14.

50 John Howard, "Prime Minister's Address to the Nation," *Prime Minister of Australia News Room* (March 20, 2003), http://www.pm.gov.au/news/speeches/speech79.html.

51 Inspector-General of Intelligence and Security, *Annual Report 2005-2006*, 25 September 2006, File Reference 2005/125, 22 http://www.igis.gov.au/annuals/05-06/pdf/IGIS_AR_2005-06.pdf.

52 Nicholas Grono, "Australia's Response to Terrorism," *Studies in Intelligence*, 48, no. 1 (2004): 28; http://www.cia.gov/csi/studies/vol48no1/article03.html.

53 Australian Government, *Protecting Australia Against Terrorism 2006: Australia's National Counterterrorism Policies and Arrangements* (2006), 40-41; http://www.dpmc.gov.au/publications/protecting_australia_2006/docs/paat_2006.pdf.

54 Director-General of Security, *ASIO Report to Parliament 2005-2006*, September 2006, Reference no. eA1004090, viii, 42; http://www.asio.gov.au/Publications/comp.htm. Under Australia's *ASIO Legislation Amendment Act 2006*, ASIO possesses special warrant powers to initiate questioning and detention for particular circumstances under the review of the Attorney General.

55 Australian Government, *Protecting Australia Against Terrorism 2006*, 40.

56 Grono, "Australia's Response to Terrorism," 27.

57 Australian Government, *Protecting Australia Against Terrorism 2006,* 8.

58 Ibid., 13.

59 Mark Thomson, *Jane's Terrorism & Security Monitor* (London: Jane's Information Group, 2006), 1.

60 Inspector-General of Intelligence and Security, *Annual Report 2005-2006*, 52.

61 Director-General of Security, *ASIO Report to Parliament 2005-2006*, 51.

62 Australian Government, *Protecting Australia Against Terrorism 2006*, 16.

63 Chalk and Rosenau, *Confronting the Enemy Within*, 49.

64 Australian Government, *Protecting Australia Against Terrorism 2006*, 42.

65 Chalk and Rosenau, *Confronting the Enemy Within*, 40.

66 Australian Government, *Protecting Australia Against Terrorism 2006*, 41-42.

67 Ibid., 24.

68 Gregory, "Intelligence led Counter-terrorism," 4.

69 Chalk and Rosenau, *Confronting the Enemy Within*, 50.

70 Manmoham Singh, "Interview of Prime Minister Dr. Manmoham Singh," interview by Charlie Rose, *Charlie Rose Show* (21 September 2004), http://www.indianembassy.org/pm/pm_charlie_rose_sep_21_04.htm.

71 Jane's Intelligence Digest, *Jane's Sentinel Security Assessment: South Asia - India: Security And Foreign Forces* (London: Jane's Information Group, 2006), 29.

72 Maloy Krishna Dhar, *Open Secrets: India's Intelligence Unveiled* (New Dehli, India: Manas Publications, 2005), 11.

73 Ministry of Home Affairs, *Annual Report 2006-07* (Government of India: 2007), 28, 31-32; http://mha.nic.in/Annual-Reports/ar0607_Eng.pdf.

74 Sarath Ramkumar, "Intelligence Agencies: Need for greater attention by the government," *Institute of Peace & Conflict Studies*, no. 579 (17 September 2001): 1; http://www.ipcs.org/newKashmirLevel2.jsp?action=showView&kValue=909&subCatID=null&mod=null.

75 Jane's Intelligence Digest, *Jane's Sentinel Security Assessment: South Asia - India: Security And Foreign Forces*, 28.

76 Rahul Bedi, "Indian intelligence gathering undermined by budget cuts," *Jane's Intelligence Review* (1 July 2004): 2.

77 Praveen Swami, "Handicapped Intelligence," *Frontline* 21, no. 14 (July 2004): 1; http//www.hinduonnet.com/fline/fl2114/stories/ 20040716001204900.htm.

78 Rahul Bedi, "Indian security shake up," *Jane's Intelligence Review*, (4 May 2001): 2; Praveen Swami, "A new intelligence organisation," *Frontline* 19, no. 6 (March 2002): 2; http://www.hinduonnet.com/fline/fl1906/19061240.htm.

79 Praveen Swami, "Bureaucrats kill critical intelligence reforms," *The Hindu,* June 18, 2004, p.1; http://www.hinduonnet.com/ thehindu/2004/06/18/stories/2004061805171100.htm.

80 Bedi, "Indian intelligence gathering undermined by budget cuts," 2; Praveen Swami, "Stalled reforms," *Frontline* 20, no. 9 (April/May 2003): 5; http://www.hinduonnet.com/fline/fl2009/stories/20030509002108700.htm.

81 Swati Pandey, *Law and Counterterrorism: The Prevention of Terrorism Act in a Strategic Dimension*, Institute of Peace & Conflict Studies Research Papers (April 2004), 4; http://www.ipcs.org/IRP04.pdf.

82 Government of India, Parliament, *Prevention of Terrorism Act, 2002* (March 28, 2002), Bill No. 5-C of 2002; http://rajyasabha.nic.in/bills-ls-rs/5-c-2002.pdf.

83 Jane's Intelligence Digest, *Jane's Sentinel Security Assessment: South Asia - India: Security And Foreign Forces*, 39; Pandey, *Law and Counterterrorism*, 5. Pandey highlighted the use of the *POTA* legislation to target political opponents.

84 Pandey, *Law and Counterterrorism*, 9. See pages 9-12 for the importance of linking law to national strategy.

85 Raman, *Intelligence: Past, Present, and Future*, 358-359.

86 Saikat Datta, "There Are No Secrets Here," *New Delhi Outlook*, 19 November 2006, p.1; http://www.outlookindia.com. The Joint Intelligence Committee had merged with National Security Council Secretariat in 1998, but was reformed into its own separate entity.

87 Bhashyam Kasturi, "The Intelligence Secret," *Institute of Peace & Conflict Studies*, no. 589 (27 September 2001),: 1;

http://www.ipcs.org/newKashmirLevel2.jsp?action=showView&kValue=899&subCatID=null&mod=null; Bedi, "Failures prompt India to reform intelligence service," *Jane's Intelligence Review* (23 May 2001), 3.

88 Dhar, 15.

89 Bedi, "Failures prompt India to reform intelligence service," 7.

90 George Iype, "Why intelligence fails, and terrorists succeed," *Rediff* (20 July 2006), p.1; http://www.rediff.com/news/2006/jul/ 20george.htm (accessed on January 4, 2007).

91 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, 23-24. Stability in organizational relationships and intelligence sharing processes is touted as a significant strength of the British system where these functions have been allowed to mature over time.

92 Swami, "Bureaucrats kill critical intelligence reforms," 2.

93 Kasturi, "The Intelligence Secret," 1.

94 Sarath Ramkumar, "Revamping of Intelligence Apparatus," *Institute of Peace & Conflict Studies*, no. 328 (22 February 2000): 1; http://www.ipcs.org/newKashmirLevel2.jsp?action=showView&kValue=641&subCatID=null&mod=null

95 Ramkumar, "Intelligence Agencies: Need for greater attention by the government," 1.

96 Swami, "Handicapped Intelligence," 4.

97 Dhar, *Open Secrets: India's Intelligence Unveiled*, 83.

98 Swami, "Stalled reforms," 4.

99 Sarath Ramkumar, "KRC: Government's Success, but Intelligence Failure," *Institute for Peace & Conflict Studies*, no. 392 (30 July 2000): 2; http://www.ipcs.org/newKashmirLevel2.jsp?action=showView&kValue=1036&subCatID=null&mod=null.

100 Bedi, "India's security shake up," 2.

101 Saikat Datta, "War Below the Radar," *New Delhi Outlook*, 31 July 2006, p.1; http://www.outlookindia.com.

102 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 395.

103 U.S. Congress, Senate, *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458 (Washington DC: GPO, December 17, 2004), 3644; http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.108.pdf. Section 101(a) established the Office of the DNI. The act also codified the NCTC. Congressional Research Service, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress* (Washington DC: The Library of Congress, August 4, 2004), 5-6; http://www.fas.org/irp/crs/RL32336.pdf.

104 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington DC: GPO, March 31, 2005), 30; http://www.wmd.gov/report/wmd_report.pdf. The report specifically called for the consolidation of the FBI's counterterrorism and counterintelligence function under the Directorate of Intelligence. It also identified several other shortfalls with the FBI's progress in transforming its organizational culture and intelligence reforms. See Chapter 10 of the report for further details.

105 Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States: Transformation through Integration and Innovation* (Washington, DC: GPO, October 2005), 1. The strategy highlights the necessity of integrating foreign and domestic intelligence efforts to eliminate the traditional gap in U.S. national security efforts.

106 Dhar, *Open Secrets: India's Intelligence Unveiled*, 13-14, 84-85. Dhar highlights these challenges for the Intelligence Bureau.

107 U.S. Congress, House, Committee on Homeland Security, *Statement of Kenneth Bouche, Colonel, Illinois State Police Regarding a Hearing on "State and Local Fusion Centers and the Role of DHS"* (September 7, 2006), 4; http://www.fas.org/irp/congress/2006 _hr/090706bouche.pdf.

108 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 419.

109 The Markle Foundation, *Protecting America's Freedom in the Information Age*, 107.

110 U.S. Congress, Senate, *Catching Terrorists: The British System versus the U.S. System*, 37.

111 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 423.

112 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 459. The DNI is chartered to exercise greater oversight since the creation of the National Security Service.

113 Posner, *Remaking Domestic Intelligence*, 37.

114 Pillar, "Intelligence," 134.

115 Kate Martin, "Domestic Intelligence and Civil Liberties," *SAIS Review* 24, no. 1 (Winter-Spring 2004): 12.

116 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 423.

117 Netanyahu, *Fighting Terrorism,* 138. Netanyahu highlights the sharing of basic, or raw data, versus the sharing of intelligence warning. He highlights the fact that basic data is often not shared between intelligence agencies of the same government due to the need to protect the information's source or from outright organizational jealousy.

118 Permanent Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*. This study identified many of the foreign-domestic intelligence sharing shortfalls, the inability of the intelligence community to provide assessments, and particularly the FBI's shortfalls in intelligence.