



HOMELAND SECURITY ADVISORY COUNCIL

**REPORT OF THE
FUTURE OF TERRORISM
TASK FORCE**

January 2007

January 25, 2007

To: Honorable Michael Chertoff, Secretary, Department of Homeland Security

From: Honorable Lee Hamilton, Chairman
Frank J. Cilluffo, Vice Chairman

Subject: Findings and Recommendations of the Homeland Security Advisory Council, Future of Terrorism Task Force

At your direction, a Future of Terrorism Task Force comprised of members of the Homeland Security Advisory Council (see Attachment A), was tasked to address the following:

- assess future threats to the United States over the next five years;
- strategically fine-tune departmental structures and processes to meet those threats; and
- recommend how to better engage and prepare the American public for present and future challenges.

The task force has consulted with key subject matter experts, from the public and private sectors, both domestic and international (see Attachment B). Briefings and discussions with these experts yielded a range of findings on trends and best practices, garnered through their experiences as they address challenges specific to their jurisdictions. It was not within the purview of the task force to undertake an exhaustive and in-depth examination of particular threats and the sources from which they emanate. Further, we cannot forecast the nature of the next attack, or when and where it may occur. Nonetheless, based upon our work over the past five months, members believe that there is every indication that the number and magnitude of attacks on the United States, its interests and its allies will likely increase. Like crime or disease, terrorism should be conceived as a chronic problem requiring a sustained and patient strategy, with ever evolving tactics.

In short, much like a successful boxer, we must keep our guard up, while maintaining speed, agility, stamina and strength to defeat our opponent. As you aptly stated on the second anniversary of becoming Secretary of Homeland Security, the challenge “is to clearly articulate a philosophy for leadership of the department that is intelligible and sensible, not only to the members of the department itself, but to the American public.” It is our hope that the findings and recommendations that follow will assist you and your colleagues to achieve this goal, in collaboration with the multitude of partners crucial to homeland security.

Findings

- *There is every indication that the number and magnitude of attacks on the United States, its interests and its allies will likely increase.*
- *Terrorism is a tactic that can be employed by any adversary. We must be prepared to respond to potential threats from unexpected as well as familiar directions.*
Globalization has changed the way we communicate, learn, and do business, but the benefits of globalization are not restricted to the benevolent. Globalization has also changed the ways our enemies can operate. Terrorism is a tool that can empower micro-actors to have a macro-impact, increasing the range of potential adversaries with the capability to do us harm.
- *The future of terrorism will depend, in large part, on the use and accessibility of technology.* Increasingly destructive weaponry makes terrorism more lethal; advances in transportation increase the reach of terrorists; and cheaper and more secure means of communication make terrorism harder to detect. As these technologies advance, proliferate and become available to a wider range of actors, more and more potential enemies may use terrorism as a strategy and tactic.
- *The future of terrorism will be affected in part by the mobility of people.* Globalization entails greater mobility in goods, services, and people, as well as money and information. Expanding markets and cheaper, easier, and faster transportation increasingly blur national borders. Whether this trend accelerates or decelerates will have a major impact on the reach of terrorist groups, and the role of national borders in security thinking.
- *The future of terrorism will be shaped by our actions in defending against terrorism.* Our adversaries base their actions in part on our actions – if we harden one target or defend against one means of attack, it pushes them to search for other vulnerabilities, redirecting the threat and displacing risk to a new area to secure.
- *Understanding the future of terrorism requires our understanding trends and developments in a wide range of areas.* It is impossible to predict with precision the future success of our adversaries, but we can evaluate the factors that will contribute to their success or failure. Among those factors are the quality of the leadership of terrorist organizations, the effectiveness of U.S. counterterrorism efforts, the availability of safe havens to the enemy, the status of political reform toward open and accountable governments in relevant regions, and many other areas. The National Intelligence Estimate (NIE) adjudges that “[g]reater pluralism and more responsive political systems in Muslim majority nations would alleviate some of the grievances jihadists exploit.”
- *The most significant terrorist threat to the homeland today stems from a global movement, underpinned by a jihadist/Salafist ideology.* The members of this movement seek to overturn regimes considered to be apostate; to re-establish the

Caliphate; and to impose an extremist, militant interpretation of Islam. Some have cast the struggle within the Muslim world over interpretation of the Qur'an as a battle for the "soul of Islam." Other extremists have grievances and aims that are more localized.

- *The core of al Qaeda is resilient and resurgent, and remains a threat to the United States.* We cannot dismiss the possibility that this group, operating out of safe havens in Pakistan and elsewhere, will succeed in executing large-scale, spectacular, mass casualty attacks against the United States and our interests abroad. However, "al Qaeda Classic" is a degraded entity with many of its remaining key figures on the run.
- *Looking to the future, a more pressing threat will be the wider movement spawned by al Qaeda and inspired and motivated by its ideology.* Al Qaeda has franchised itself across the globe, with its franchises prepared to act locally, and largely independently – in effect a network of networks. Attacks on the United States, its interests, and its allies, are seen as a means to accomplish these ends. We have seen the recent emergence of a leaderless movement, marked significantly by self enlistments, to include "homegrown" terrorists taking its inspiration from "al Qaeda Classic" to join the global Salafi jihad, or to act on more local grievances.
- *While difficult to measure with precision, it is known that al Qaeda's ideology is spreading.* Per the National Intelligence Estimate, "Although we cannot measure the extent of the spread with precision, a large body of all-source reporting indicates that activists identifying themselves as jihadists, although a small percentage of Muslims, are increasing in both number and geographic dispersion." It should be remembered that the enemy is not monolithic, nor wholly Islamic. It should also be noted that the enemy does not target non-Muslims exclusively. Indeed, al Qaeda and other extremists are indiscriminate in their targeting, and a significant number of their victims have been Muslim.
- *It is important to remember that the threat of state-sponsored terrorism will not disappear.* Concerns have been expressed, for example, about Iranian support for Hezbollah, and the implications for U.S. national security should tensions with Iran escalate further. The same concerns regarding Hamas and the Palestinian-Israeli issue must be considered as well. As this report has stated, terrorism is a tactic and the proven successes of these tactics may very well be utilized by nation states hostile to the U.S. inside our borders.
- *The Internet has become a major facilitator of terrorist activities, especially the spread of jihadist ideology.* The internet facilitates almost every aspect of terrorist activities, from training and fundraising to communications and planning. But more importantly, the internet provides a powerful tool for extremists to spread their message and thereby spur both recruitment and self-enlistment into the jihadist movement. Chat rooms, videos circulated widely via the Web, and other online forums and tools – all used to best advantage by a technologically sophisticated foe –

fuel the movement by keeping “believers” energized through graphic images, language and even song, and inspiring others to join the cause. As pointed out to the task force, the use of virtual training camps on the internet is replacing the typical training camps that have been used in the past, thus reaching a much wider audience and limiting the intelligence communities’ abilities to track individuals transiting into these camps.

- *The alienation of Muslim populations in the Western world is a major component of the spread of jihadist ideology.* Muslims living in the United States are on balance more integrated, more prosperous and therefore, less alienated than Muslims living in Western Europe. The relative socioeconomic marginalization of Muslim communities in Europe renders them more vulnerable to radical political and religious messages. While by comparison the United States is in a privileged situation, we are not immunized against the challenge, as borders are not the firewall that they once were. Muslim culture, and in particular the Islamic faith, are not widely understood within the Western world. This lack of understanding, coupled with fear of extremist adversaries, taints our ability to relate with the larger and overwhelmingly peaceful and moderate Muslim population, reinforcing misconceptions of and dividing us from those susceptible to radicalization.
- *The evolving complexity of our adversaries challenges existing paradigms – walls separating state, local, and federal responders are counterproductive, and the bifurcation of homeland security from national security is no longer relevant.* The potential rise of self radicalized, unaffiliated terrorists domestically cannot be easily prevented through traditional federal intelligence efforts, and requires the incorporation of state and local solutions. Similarly, the protection of critical assets, as well as the initial response to an attack, are primarily state, local and private sector responsibilities, with federal assets and resources provided as a supplement. Los Angeles County, the City of Los Angeles, and Orange County of California provide one example of a strong model for the rest of the nation. Both before and after September 11, Los Angeles and Orange Counties created working groups with their federal, state, local and private sector partners to share information and to work on preparedness issues. Their experience in responding to natural disasters has provided the structured organization for emergency and disaster management. Although progress has been made in moving towards a goal of a seamless coordination capability between federal, state and local authorities to ensure homeland security, there are still gaps in this coordination that must be closed. The Task Force was encouraged by the Director of Intelligence’s initiative to staff state fusion centers with DHS analysts. This program will prove to be valuable not only in information sharing, but educating state and local agencies on what they should be looking for and reporting.
- *Continuous learning is required – especially from allies abroad – as the threat will continue to evolve.* U.S. friends and allies have much to offer. Australian officials, for example, have concluded that protective security measures over the next five years must not become rigid, and both variability and unpredictability must be

consciously injected into flexible prevention measures. Israeli officials highlighted the need for public participation, rather than just awareness, and emphasized that resilience must be built from the bottom up in addition to the top down. In Britain, officials have worked to inculcate in the public an understanding that there is no such thing as zero risk, and that sometimes even the best efforts of the authorities will not be good enough.

- *Just as Al Qaeda has demonstrated their flexibility and capability to adapt their tactics and procedures due to new policies and protective measures, we must maintain the same level of flexibility, unpredictability and not etch in stone certain policies and organizational structures of the department.*
- *We cannot protect everyone, everywhere all the time – understanding mitigates the “terror” in “terrorism.”* Terrorism targets the psychological, as well as the physical, well-being of our populace; the fear generated by unpredictable attacks is a key goal of terrorism. The range of threats we face is too diverse, too deadly, and in some cases (as in domestic terrorism) often too difficult to detect before an attack, to secure every target completely. The public has yet to fully internalize this reality. It is critical that DHS enlist the American public in efforts to prepare for current and future threats through education and the communication of consistent, trustworthy messages that realistically, comprehensibly and persuasively convey these risks, including the ambiguity about when, where, and how an attack will occur. There is little evidence that the public will “panic” with this information. Instead, evidence suggests that the public often adapts and cooperates with trusted officials.

Recommendations

As Abraham Lincoln said in a message to Congress on December 1, 1862: “As our case is new, so we must think anew, and act anew.” To get ahead of future threats, our strategies and resulting tactics need to be informed by a more fulsome understanding of the nature of our adversaries. We have a tendency to fight yesterday’s wars – with the same weapons, tactics and mindsets employed previously with great success (e.g., the Cold War). While there are lessons to be drawn from the past, countering this new global insurgency requires a paradigm shift. Our adversary is proactive, innovative, well networked, flexible, patient, young, technologically savvy, and learns and adapts continuously based upon both successful and failed operations around the globe. We must be and do likewise. Our institutions must be recalibrated to reflect the changing threat environment. Therefore we recommend the following:

Policies, Programs and Procedures

The Secretary should establish an Office of Net Assessment (ONA) within the Department to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats.

The range of existing threats and crises already facing the U.S. leaves the homeland security community with little time to prepare for threats that have not materialized.

Rather than focusing on current threats and responses, the primary role of the ONA would be to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats. The ONA would fill the much-needed role of producing long-term assessments and strategy, acting as a brain trust of creativity and imagination. In order to accomplish this tall order, the duties of ONA would include:

- studying existing threats in order to project their evolution into the future;
- studying trends in the weapons, technologies, modalities, and targets utilized by our adversaries (i.e., the events that can transform the security landscape);
- reviewing existing US. capabilities in order to identify gaps between current capabilities and the requirements of tomorrow's threats;
- conducting war games and red team scenarios to introduce innovative thinking on possible future threats;
- assessing how terrorist groups/cells could operate around, and/or marginalize the effectiveness of, policies and protective measures.

The ever-shifting and unpredictable security environment facing the U.S. requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable. The ONA, on which this task falls, must take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, and other trends.

The Secretary should conduct a comprehensive, systematic, and regular examination – a Quadrennial Security Review – of all homeland security threats, assets, plans and strategies with a view toward long-term planning and modernization.

The department must be able to respond to a wide range of unforeseen threats that will arise rapidly presenting little time to develop ad hoc responses. A systematized and regular process of reviewing all threats, resources, and plans would allow the Secretary to shape a homeland security capability that is robust, flexible, and adaptable before a threat materializes. Simply put, a QSR would allow the Secretary to determine what the threats are, what tools are needed for meeting them, what force structure is needed (at the federal, state and local levels), and what resources are needed from Congress to make that plan a reality. This concept will better facilitate a requirements-based approach within the department's budget process. The Secretary will review the national homeland security strategy, the Department's existing resources, structure, transformation plans, infrastructure, budget plan, modernization plans, and other elements of the homeland security programs and policies of the United States. In order to prepare for the full scope of potential threats, the Secretary must consult with other agencies, including the Department of Defense, the Department of Health and Human Services, the Department of Justice, the Department of State, the Department of the Treasury, Federal Bureau of Investigation, the Intelligence Community, state and local officials, private sector partners, international partners, and other relevant agencies.

The Secretary should undertake, in conjunction with the Director of National Intelligence (DNI), a comprehensive National Intelligence Estimate to address threats to the homeland, both foreign and domestic.

Potential threats to U.S. security do not just originate overseas, and an effective review must include possible domestic threats. At present, work is underway on a NIE for the Homeland, which is informed by a Deputy National Intelligence Officer (DNIO) from the FBI. This development is to be commended. However, within the National Intelligence Council (NIC), there is no deputy level representative from DHS, which means that a domestic threats security perspective, including systematic input from state and local officials, is not fully provided. Moving forward, state, local and private sector input must drive the domestic component of the assessment, and must be continually updated. Concomitantly, structures must be put in place (including state fusion centers) to develop and apply indicators that weed out signal from noise. Further, the DNIO position should become permanent and rotate between FBI and DHS.

Countering “home-grown” radicalization must be one of the Department’s top priorities by using the Department’s Radicalization and Engagement Working Group (REWG) to better understand the process – from sympathizer to activist to terrorist.

Current efforts of the REWG within the Office of Strategic Plans to this end should be done in coordination with the NIE mentioned above. The REWG should be directed to develop a set of radicalization metrics (separate from terrorism metrics) for law enforcement and intelligence reporting that would function as an early warning system, detailing where radicalization may be occurring and/or increasing. Such a warning system could be used to: target civic engagement and de-radicalization programs; guide further intelligence collection; and inform terrorism risk assessments underpinning resource allocations, such as UASI funding. Collectively, this process will produce proactive strategic intelligence to identify emerging home-grown terrorism trends.

The Department must place a renewed emphasis on recruiting professionals of all types with diverse perspectives, worldviews, skills, languages, and cultural backgrounds and expertise.

The vast cultural differences between Muslim communities and the West create difficulties and missed opportunities. The Department, the federal government, particularly the intelligence community, must have diverse perspectives to approach this issue. The Department must make an effort to recruit individuals who have all types of cultural backgrounds, language and unique perspectives that can address the challenges we face. In addition, greater cultural understanding by all department employees will assist in creating a stronger relationship with the Muslim community. This also applies to the US counter-terrorism community as a whole.

Cultural and Religious Awareness and Understanding – Action Items

The Department should work with subject matter experts to ensure that the lexicon used within public statements is clear, precise and does not play into the hands of the extremists.

Our use of language, both within government and the media, is insufficiently nuanced to convey the multidimensional aspects of Islam. This lack of sophistication has caused us to adopt the very lexicon that al Qaeda and its affiliates would prefer we use, in order to further their aims and objectives. Whoever controls the ‘war of words’ influences the outcome of the battle of ideas. Therefore, DHS must work with subject matter experts to ensure that the lexicon used within public statements is clear and precise, and does not play into the hands of the extremists. This effort must include other governmental entities if it is to be effective.

Broader avenues of dialogue with the Muslim community should be identified and pursued by the Department to foster mutual respect and understanding, and ultimately trust.

To change hearts and minds – and encourage moderation – we must challenge ideas with ideas. Trust is the most valuable currency we have in this battle because trust underpins all counterterrorism tools (e.g., military, diplomatic/policy, legal, economic and covert action).

Local communities should take the lead on developing and implementing Muslim outreach programs. DHS should encourage and support with appropriate resources outreach efforts and facilitate the sharing of best practices.

Several western governments are currently developing and implementing Muslim outreach programs. The Task Force is split on what the ideal level of governmental involvement should be in such efforts. Consensus was reached on the need for individual communities to take the lead in these efforts. Messages must be delivered by existing credible sources within Muslim and diaspora communities nationwide. The role of DHS in this effort is seen to be one of encouraging such outreach, dialogue and inclusion efforts. While each community is unique, there may be models and initiatives that could be highlighted to assist religious, educational and cultural community-based organizations in these efforts.

DHS in support of State, Local and Private Industry Efforts

The Secretary should work directly with state, local, private sector and community leaders to educate them on the threat of radicalization, the necessity of taking preventative action at the local level, and to facilitate the sharing of other nations’ and communities’ best practices.

The evolution of home-grown terrorism in Europe and other parts of the world is a warning signal to America that must be heeded. Solutions and practices to address the potential for radicalization must be developed by local communities – not directed by Washington. As part of these community-based efforts aimed at mutual understanding and elimination of conditions that allow extremist ideologies to take root, the Secretary should assume the role of “catalyst” in order to incentivize state and local authorities to proactively address the potential for radicalization before home-grown terrorism evolves. Specifically, the Secretary should actively work directly with Mayors, Governors, and community leaders to educate them on the threat of radicalization, and to share best practices information from communities and other nations that have aggressively engaged this threat.

The Department should move immediately to implement the recommendations contained in earlier HSAC reports on information sharing.

This should include resolving issues such as classification of information, as well as ensuring that appropriate resources and standards are in place to ensure consistency and adequacy in analytical training and capabilities in fusion centers around the country.

Recognizing that successful information sharing with state and local authorities as well as the private sector requires a federal government-wide effort, the Secretary should continue efforts to support the establishment of the Information Sharing Environment. DHS should ensure that information sharing capability between the private sector, local, state, regional and federal governments is developed according to consistent standards and founded upon a formal requirements process. Your recent decision to support and provide guidance for the establishment of fusion centers, and to increase the number of federal personnel assigned to work alongside state and local authorities in fusion centers, is laudable. The continuing issue of classification of information inhibiting the exchange of critical information between federal, state, local authorities and the private sector must be solved.

State and local capability to gather, process and share information within local regions and with the federal government must remain a priority, and should be developed through an operational partnership with the federal government, ensuring that training, analytical capability, and resources are consistent and meet the overall national need. The Secretary should continue efforts with state and local authorities to build regional operating capabilities and plans for prevention, protection and response by requiring DHS components to develop their plans and capabilities in concert with state and local authorities. DHS should also make federal resources to state and local authorities contingent upon regional collaboration.

The Task Force notes that the evolution of terrorism in other countries continues to focus on attacks on key infrastructure, in particular transportation. While much of the current requirement to protect critical infrastructure falls upon state and local authorities and the private sector, DHS should continue to work in collaboration with state, local and private sector leaders to ensure the resiliency and reduce the vulnerabilities of key critical

infrastructure, all the while taking into account international experience. Using a risk-based approach, the Secretary should bring appropriate federal authorities, the private sector, and state and local government to the table to reach agreement on a long-term plan to address the vulnerabilities of key U.S. critical infrastructure.

Separate and distinct from these efforts, DHS should work through its traditional channels of coordination with state and local authorities to ensure that actionable information on the threat of radicalization, as well as practices for addressing the threat, are provided.

The Department should develop and immediately implement, in concert with the Department of Justice and state and local corrections officials, a program to address prisoner radicalization and post-sentence reintegration.

A great deal of radical literature is distributed in state prisons. Prisoners are by definition an estranged “captured audience” for indoctrination into radical movements. Even in prison, inmates can continue to radicalize through mail and the internet. Prisoners are also exploiting civil rights laws behind bars to justify radicalization activity. There is great potential to de-radicalize prisoners through monitoring and rehabilitation at the time of their re-entry into society. This issue must be incorporated into the entire “correctional system” to include awareness on the part of parole officers who can provide critical information on a former inmate who has become radicalized in prison. It would be beneficial to state correctional officials to have some form of training documents or guidebook prepared jointly by the Department and the Department of Justice.

International Implications

The Department must use all avenues of international cooperation and instruments of statecraft to boost existing and form new partnerships to foster and maintain a global network that permits, among other things, robust intelligence and information sharing.

A military approach alone will not suffice to meet and combat future threats. In this battle, we must balance and integrate all elements of statecraft, including diplomatic, economic and legal instruments. The enemy – its leaders and safe havens, and the conditions (e.g., political, social, cultural) that it exploits – must be engaged and defeated holistically. DHS officials must therefore be trained to think in these terms, and to fully appreciate the nuances between and among the different levels of the battlefield, from the local to the national to the regional to the global. Moving forward, it is imperative that we learn from experiences elsewhere in order to better prevent, prepare for, and respond to attacks, and the ever changing means and modes of the enemy.

Although the operational tends to overtake the strategic in the course of the daily grind, we must not become overwhelmed or complacent. DHS must look outward and build and cultivate its own “network of networks” by strengthening nascent efforts to engage with, learn from and share best practices among the worldwide community of homeland security professionals. If we are to penetrate and destroy the adversaries’ web of

networks, the density, richness and complexity of our own global networks must match and outpace theirs. Such a network exponentially increases our ability to develop the ‘imagination’ and knowledge base required for successful awareness and prevention efforts in the United States and among our allies.

Our level of success in meeting our mission will be directly linked to our current and future partnerships. As intelligence feeds all the instruments of statecraft, it is crucial that DHS and other U.S. entities foster and maintain a global network that permits robust intelligence and information sharing. U.S. ambassadors can help expand and reinforce crucial international linkages, but must be trained to become better versed in matters of homeland security. The most important long-term task is not eradicating malign networks; it is building legitimacy and the rule of law in the nations that need it most.

Public Engagement: Communicating Trustworthy and Accurate Messages

The Department should partner with the media and educational institutions to engage the public in prevention and response efforts – developing consistent, accurate, realistic, persuasive and actionable messages as well as evidence-based strategies for communicating the same.

It is critical that the American public become engaged in understanding and preparing for terrorism. Over the next five years, the public must learn about the choices faced by the nation, communities, families, and individuals. It must become a partner with its government, sharing the burden. For that to happen, it is vital that DHS be seen as trustworthy. DHS will need to work with multiple messengers, trusted within diverse communities, to effectively communicate its messages. Additionally, it will require DHS communications to be scientifically sound and rigorously evaluated.

As we move to a new paradigm, civil liberties and individual rights must be preserved – the cure must not be worse than the disease. If we are to maintain the values upon which this Nation was founded, a certain amount of risk must be accepted.

In partnership with the media and educational institutions, DHS should:

- Develop consistent and trustworthy messages that realistically, truthfully, comprehensibly and persuasively convey the risks we face, along with the ambiguity about when, where, and how those risks might materialize.
- Maintain credibility and public trust by keeping the public fully informed and by providing accurate, science-based information.
- Provide clear, concrete recommendations for personal safety actions – both during and following crisis – that enable a choice of options (if available) and enhanced perceptions of control.

- Identify evidence-based strategies for communicating these messages and involve psychologists in the shaping and empirical evaluation of communications.
- Continue to engage the media as an ally in the timely dissemination of accurate and actionable information. To do so will involve improving media relations *in advance of a crisis*, sharing information, and working aggressively to minimize suspicion and mistrust. Effective crisis communication strategies and plans at all levels of government and within the private sector should be developed in collaboration with one another and respective media outlets. (It should be noted that similar recommendations concerning the role of the media were detailed in the Private Sector Information Sharing Task Force Report, August 2005.)
- In collaboration with the Department of Education and state and local partners, consideration should be given to implementing developmentally appropriate education at the elementary school, high school and college/university levels.

Integrating National Security and Homeland Security Policy

Consider naming the Secretary of Homeland Security to the National Security Council in order to fully integrate national security with homeland security.

Homeland security and national security are inextricably intertwined. At the interagency level, the bifurcation of homeland security from national security is not helpful. To undertake a truly comprehensive national intelligence assessment, both perspectives must be integrated. To use the classic boxing analogy, we can't drop our left when we throw our right. The current practice is to engage the Secretary in National Security Council (NSC) discussions and deliberations on an ad hoc basis, which risks acting in a global environment without the full picture. In today's world it must be understood that U.S. military actions abroad and foreign policy will most likely have a spill over effect within the borders of our country. We therefore recommend that consideration be given to fully integrating the domestic security perspective in the work of the NSC by naming the Secretary of Homeland Security to the NSC. Further, the Task Force deliberated the advisability of merging the NSC and the HSC; however, consensus was not reached on this matter. Action on the recommendation to appoint the DHS Secretary to the NSC is beyond the Secretary's authorities.

Attachment A

Task Force Members

Honorable Lee Hamilton, Director, Woodrow Wilson International Center for Scholars
(*Task Force Chair*)

Frank Cilluffo, Associate Vice President for Homeland Security, The George Washington University (*Task Force Vice-Chair*)

Kathleen Bader, Textron Inc., Board Member

Elliott Broidy, Chairman and CEO, Broidy Capital Management

Dr. Roxane Cohen-Silver, Professor of Psychology and Social Behavior, University of California, Irvine

Dr. Ruth David, President and CEO, ANSER

James Dunlap, President, Dunlap Consulting (Former Oklahoma State Senator)

Honorable Thomas Foley, Partner, Akin, Gump, Strauss, Hauer, Feld

Steve Gross, President, BiNational Logistics LLC

Glenda Hood, Chairman, Glenda Hood Consulting (Former Secretary of State, State of Florida)

Don Knabe, LA County Board of Supervisors

John Magaw, Former Under Secretary for Security, U.S. Department of Transportation

Patrick McCrory, Mayor, Charlotte, North Carolina

Bill Parrish, Associate Professor, Homeland Security and Emergency Planning, Virginia Commonwealth University

Mitt Romney, Former Governor, Commonwealth of Massachusetts

James Schlesinger, Chairman, Board of Trustees, The MITRE Corporation (*HSAC Vice-Chair*)

Jack Skolds, President, Exelon Energy Delivery and Exelon Generation

Dr. Lydia Thomas, President and CEO, Mitretek Systems Inc.

Judge William Webster, Partner, Milbank, Tweed, Hadley & McCloy, LLP (*HSAC Chair*)

Houston Williams, Chairman and CEO, Pacific Network Supply Inc.

Allan Zenowitz, Former Executive Officer, FEMA

Homeland Security Advisory Council Staff

Doug Hoelscher, Executive Director, Homeland Security Advisory Committees

Michael Fullerton, Deputy Executive Director, Homeland Security Advisory Committees, Director/Future of Terrorism Task Force and Director/Academe and Policy Research Senior Advisory Committee

Candace Stoltz, Director/Future of Terrorism Task Force, Director/Private Sector Senior Advisory Committee

David Baker, Associate Director/Future of Terrorism Task Force, Intelligence Analyst

Mike Miron, Director/State and Local Officials Senior Advisory Committee

Ruth Smith, Special Assistant

Carnes Eiserhardt, Executive Assistant

Kezia Williams, Conference Coordinator

Attachment B

Subject Matter Experts

Javed Ali, Senior Intelligence Officer, DHS
Sheriff Lee Baca, Los Angeles County, California
Randy Beardsworth, Assistant Secretary for Strategic Plans
Gina Bennett, Deputy National Intelligence Officer, Transnational Threats, Office of the Director of National Intelligence
Chief William Bratton, Los Angeles Police Department
Frank Buckley, Co-Anchor, KTLA Prime News, Los Angeles, California
Sharon Cardash, Associate Director, Homeland Security Policy Institute, The George Washington University
Sheriff Michael Carona, Orange County, California
Joel Cohen, Intelligence Liaison Officer, California, Department of Homeland Security
Ambassador Henry Crumpton, Coordinator for Counterterrorism, Department of State
Osborne Day
Derek Dokter, Counselor, Ministry of the Interior and Kingdom Relations, Royal Embassy of the Netherlands
Steve Emerson, Executive Director, The Investigative Project on Terrorism
Eric Fagerholm, Acting Assistant Secretary for Strategic Plans, DHS
Richard Gerding, Counselor for Police and Judicial Affairs, Royal Embassy of the Netherlands
Jim Guirard, TrueSpeak Institute
Chris Hamilton, Senior Fellow, Counterterrorism Studies, The Washington Institute for Near East Policy

Attachment B

Subject Matter Experts

Chief Jack Harris, Phoenix Police Department

Brian Michael Jenkins, Senior Advisory to the President, Rand Corporation

Brigadier General Yosef Kuperwasser, CST International

Dr. Harvey Kushner, Chairman, Department of Criminal Justice, Long Island University

Jan Lane, Deputy Director, Homeland Security Policy Institute, The George Washington University

Tony Lord, First Secretary, Justice and Home Affairs, British Embassy

David Low, National Intelligence Officer, Transnational Threats, Office of the Director of National Intelligence

Simon Mustard, Counter Terrorism and Strategic Threats, Foreign and Security Policy Group, British Embassy

Dr. Walid Phares, Senior Fellow, Foundation for Defense of Democracies

Dennis Pluchinsky, George Mason University

Peter Probst, Consultant

Mark Randol, Director of Counterterrorism Plans, DHS

Ambassador Dennis Richardson, Australian Embassy

Dr. Joshua Sinai, Program Manager, The Analysis Corporation

Robert Spencer, Director, Jihad Watch

Dan Sutherland, Officer for Civil Rights and Civil Liberties, DHS

Major General Israel Ziv, CST International