CHAPTER 10

HOMELAND SECURITY: THE DEPARTMENT OF DEFENSE, THE DEPARTMENT OF HOMELAND SECURITY, AND CRITICAL VULNERABILITIES

Lieutenant Colonel Daniel M. Klippstein

> We look forward to working with the newly proposed organization to do everything possible to provide for our country's national defense.
>
> Donald Rumsfeld, June 2002

INTRODUCTION

Today, Americans consider themselves "a nation at war." Though the United States has experienced war, both total and limited, the nature of this particular war is one with which it has had little experience. Some have defined this conflict as a "War on Terrorism," a war whose duration will extend for many years and whose battlefields will be simultaneously abroad and within national borders. As a nation, Americans now confront the unique and unenviable task of having to conduct both strategic defensive and offensive operations. Success will depend on how well they can sustain the strategic defensive, while enduring the uncertainty of prolonged offensive actions as the U.S. military seeks to ". . . bring our enemies to justice, or bring justice to our enemies."[1]

The prosecution of this war has followed the traditional American pattern of waging war—absorb the first attack, mobilize national will, apply the necessary resources, and conduct offensive operations. America's strategy is simple—seek out and annihilate the enemy. The political and military end state is not one of limited objectives, but one consistent with total war. This war will end only when the enemy no longer has the capability or will to fight.

America's strategic, operational, and tactical actions seek to gain and retain the initiative—to take the fight to the enemy—regardless of where he lives or operates.

Executing decisive offensive operations relies upon both national will and the ability to project power from the protected borders of the United States. Yet, as Americans have discovered, their borders do not provide the necessary physical protection they have taken for granted over the past two centuries. Thus, America left a strategic center of gravity—the national will—open to attack.[2] For the first time since World War II, Americans must focus part of their national efforts on conducting strategic defensive operations.

Strategic defensive operations serve a two-fold purpose: first, to protect U.S. centers of gravity from (further) attack; second, they facilitate the uninhibited conduct of power projection in support of decisive operations. One can also term this strategic defensive "homeland security.". Viewed within the context of current joint doctrine, homeland security represents a critical capability.[3]

Today, herculean federal efforts are underway to improve the nation's homeland security by attempting to combine the efforts of a myriad of bureaucratic departments and agencies. Key to the focusing of these efforts is the relationship between the Department of Defense (DoD) and the newly formed Department of Homeland Security (DHS). This relationship represents a critical requirement, since its effectiveness is a condition that directly supports the success of homeland security and sustainment of the national will.[4] Any seams or friction within this relationship represent a critical vulnerability that terrorist can exploit to affect future attacks.[5] Therefore, a strong relationship between the DoD and the DHS reduces that vulnerability to America's homeland security and ensures the successful prosecution of the war on terrorism.

This chapter identifies several key issues that, if improperly addressed, could lead to critical vulnerabilities, since the DoD's and the DHS's relationship is not yet wholly functional. To identify potential vulnerabilities, it is first essential to address homeland security as a concept; provide an overview of the evolving roles of both departments in relation to homeland security; and relate their roles to current national strategies and statutory requirements. From this perspective, one can identify potential critical vulnerabilities

and provide recommendations to deny enemy identification and exploitation. Such recommendations require interagency coordination and approval through either the National Security Council or the Homeland Security Council. Choosing between these fora has implications for the DoD and the DHS and influences how each department will seek to reduce the identified vulnerability. Nevertheless, both departments have an obligation to the American people to identify and resolve critical vulnerabilities. The elimination of these vulnerabilities protects the United States through an effective strategic defense and enables the conduct of decisive operations in the war on terrorism.

HOMELAND SECURITY—THE WAKE-UP CALL

Before the terrorist attacks of September 11, 2001, the concept of homeland security had gained only limited attention of the federal bureaucracy. A number of studies, including those conducted by RAND, the Center for Strategic and International Studies (CSIS), and the Hart-Rudman Commission, warned of the growing threat to the homeland and recommended steps to strengthen the nation's ability to prevent and recover from a terrorist attack. A consistent theme was that the nation had not organized itself to defend against increasing levels of terrorist threats. More pointedly, it was not a question of "if" terrorist would attack the United States, but rather "when."[6] The mid-morning hours of September 11, 2001, bore out such concerns. In the wake of 9/11, Americans confronted the fact that the studies had been correct; as a nation, the United States was unprepared and vulnerable to terrorist attacks. Americans discovered that over 100 federal agencies—including DoD—shared responsibility for "homeland security," yet effective interagency coordination was lacking. A coherent strategic defense of the nation's homeland was found wanting because "the country has never had a comprehensive and shared vision of how best to achieve this goal."[7] Efforts to address this failure are generating significant requirements for the DoD.

THE NATIONAL STRATEGY FOR HOMELAND SECURITY

In July 2002, nearly 10 months after the September 11 attacks, the Bush administration developed and published the National Strategy for Homeland Security (NSHS). This strategy statement, the first ever promulgated by a U.S. President, aimed at providing a coherent national effort to improve the security of the American homeland. Its stated objectives are: (1) prevent terrorist attacks within the United States; (2) reduce America's vulnerability to terrorism; and (3) minimize the damage and recover from attacks that do occur.[8]

Establishment of critical mission areas that support the accomplishment of the above objectives is key to the strategy's execution. The NSHS establishes six critical mission areas as a framework to focus the nation's efforts: (1) intelligence and warning; (2) border and transportation security; (3) domestic counter terrorism; (4) protecting critical infrastructure, (5) defending against catastrophic terrorism; and (6) emergency preparedness and response.[9] This strategy further defines specific objectives and goals for federal, state and local agencies that are vital to a cohesive strategic defense and the security of the homeland. Executing the NSHS requires a new cabinet level department with overall authority and responsibility for accomplishing these objectives. The agency designed for this end, the Department of Homeland Security, has the responsibility of unifying national efforts for executing this strategy.

THE DEPARTMENT OF HOMELAND SECURITY

On November 25, 2002, President Bush signed the Homeland Security Act of 2002 (HSA) and thereby established the DHS. This act represents the most sweeping reorganization of the federal government since the National Security Act of 1947 established the DoD. While arguments continue over the necessity for a new department, the fact remains that consolidating responsibility for homeland security into a single agency, responsible to the president, congress and the nation, represents a significant step in creating

a strategic defense focused on protecting the nation from future attacks. Once operational, the DHS's budget of approximately $36.2B, is the eighth largest in the federal government for Fiscal Year 2004. With over 170,000 employees, it will be the third largest department of the 15 departmental cabinet positions within the government. Given its mission, budget and manpower, the DHS will be one of the most influential governmental agencies, in company with the DoD, the Department of State, the Department of Justice, and the Central Intelligence Agency.[10]

The Homeland Security Act of 2002, clearly makes the DHS responsible for the six critical mission areas of the NSHS in the following mission statement:

> (a) Prevent terrorist attacks within the United States; (b) reduce the vulnerability of the United States to terrorism; and (c) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States; (d) carry out functions of entities transferred to the Department [of Homeland Security], including acting as a focal point regarding natural and manmade crises and emergency planning…; and (g) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.[11]

To accomplish these missions, the new department will consolidate over 22 agencies from across the federal government into a new, more cohesive department. Few, if any, federal agencies will remain untouched by the reorganization, including the DoD.

This consolidation will be no small task. One of the department's greatest internal challenges will be to instill organizational identity, pride, and a common culture, while recognizing the divergent subcultures within the existing agencies. These subcultures will significantly influence development of intradepartmental relationships. They will also influence interdepartmental behavior with other agencies, including the department's participation within the interagency coordination process. In either case, forging a new organizational culture to create a synergy of efforts, internally and externally, is not achievable overnight or by the stroke of a pen. It represents a continuous process over the course of the foreseeable

future.

Organized similar to other federal departments, the DHS will have a deputy secretary, four under secretaries, numerous assistant secretaries, and directors of various subordinate agencies. Of particular importance to DoD is the Commandant of the Coast Guard and the four Departmental Under Secretaries: Information Analysis and Infrastructure Protection, Science and Technology, Border and Transportation, and Emergency Preparedness and Response. The historical interaction of the soon-to-be-subordinate agencies with DoD indicates that future coordination requirements will center on these five key functional offices. Establishing direct and effective coordination between the under secretaries and their DoD counterparts will create the essence of the critical requirement to support homeland security.

Despite its significant budget and manpower, the DHS does not have sufficient dedicated assets, including equipment and specially trained personnel, to respond independently to catastrophic events—natural or manmade—by itself. It must rely upon state and local government agencies to provide first responders for most events and depend on other departments within the federal government for specialized or unique equipment or expertise. While the Department will have to coordinate closely with other federal departments and agencies, its most critical relationship will be with the DoD. This relationship will receive increasing focus within federal and public circles, as the concept of homeland security and the role of the DHS matures.

DEFINING HOMELAND SECURITY AND DOD'S ROLE

Prior to the publication of the National Strategy for Homeland Security, there was wide spread confusion and disagreement within DoD and the federal government at large, regarding the concept and definition of homeland security. In many instances, the terms "homeland security" and "homeland defense" were mutually interchangeable. In some circles they were synonymous with national defense issues. However, the NSHS codifies the definition

of homeland security and provides a common point of reference for federal, state, and local government agencies. This definition places the relationships among various agencies, especially the Departments of Homeland Security and Defense, in perspective. The National Strategy for Homeland Security defines homeland security as: "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[12] This definition emphasizes a national, as opposed to a federal, effort to secure the homeland, and focuses those efforts on the prevention of and response to terrorism.

Within this framework, DoD provides military support to the DHS, as the lead federal agency for homeland security. However, in extreme circumstances, DoD may become the lead federal agency in securing the homeland. Regardless of its domestic support requirements, DoD simultaneously contributes to homeland security through on-going military operations overseas (e.g., Operation ENDURING FREEDOM) and overseas forward presence. DoD's actions, both at home and abroad, aim at deterring, preventing, preempting, disrupting, or destroying threats to the United States before they can reach the nation's shores.

Secretary of Defense Donald Rumsfeld established the parameters for the Department's support to homeland security by dividing his department's roles into homeland defense and civil support mission areas. He characterized the Department's operational involvement in terms of three circumstances: "extraordinary" circumstances (homeland defense), "emergency" circumstances (military assistance to civil authorities), and "limited scope" operations (military support to national special security events):

> First, under *extraordinary circumstances* that require the department to execute traditional military missions, such as combat air patrols and maritime defense operations. In these circumstances, DoD would take the lead in defending people in the territory of our country supported by other agencies. And plans for such contingencies would be coordinated, as appropriate, with the National Security Council and with the Department of Homeland Security. . . . Second is the *emergency circumstance* of a catastrophic nature. For example, responding to the consequences of attack,

> assisting in response, today, for example, with respect to forest fires or floods, tornadoes and the like. In these circumstances, DoD may be asked to act quickly to provide and supply capabilities that other agencies simply don't have . . . And third, our missions or assignments that are *limited in scope* where other agencies have the lead from the outset. An example of this would be security at special events, like the recent Olympics, where DoD worked in support of local authorities.[13] (author's emphasis)

These terms describe two critical aspects of the DoD's functions in support of homeland security. First is the temporal nature of its support, based on the severity of the event or crisis to which the Department responds. Each term implies that departmental support or activity will be temporary—focused on addressing the immediate needs that exceed the lead federal agency, state, or local capabilities in stabilizing a crisis situation. Second, these categories represent traditional areas of the Department's activity in defending the nation and providing military assistance to civil authorities in times of crisis. Collectively, these terms provide a framework within which the Department can determine and sequence its commitments in response to crises. Additionally, by defining these three circumstances, the Department can develop and refine specific operational plans for the domestic employment of military assets, across the spectrum of potential responses, always in consideration of constitutional and legal limitations.

Despite the broad statutory authority of the Department of Homeland Security, it does not have the authority to direct other federal departments, including DoD, to conduct specific functions or expend internal resources. The Secretary of Defense or the President determines, when and where to employ DoD assets. The commitment of DoD assets in any of the three circumstances, in support of the NSHS, must occur within the context of the demands of the National Security Strategy.

THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES

The National Security Strategy of the United States (NSS)

provides a broad strategy for how the United States, employing the various elements of national power, will confront a complex and increasingly dangerous strategic environment. This strategy includes a specific focus on the war on terrorism and establishes homeland security as a vital national interest.

DoD's efforts, in support of the NSS, focus on identifying and destroying threats to the nation before they can threaten U.S. borders. However, some threats, whether conventional or asymmetrical, will still evade detection, penetrate U.S. defenses, and strike critical vulnerabilities. In such circumstances, though the United States treats terrorism inside its borders as a criminal act, DoD still has a significant role. It must execute its role in coordination with the DHS to prevent and/or respond to a terrorist attack. A secure homeland is fundamental to the nation's ability to execute the requirements of its NSS.

For DoD, the complementary requirements of the NSS and the NSHS present a complex challenge in the balancing of homeland and national security obligations. Concurrently, to fulfill the broad requirements of homeland security, while "transforming" to meet future threats, the NSS requires the Department to develop a "…broad portfolio of military capabilities that must also include the ability to defend the homeland, conduct information operations, ensure U.S. access to distant theaters, and protect critical U.S. infrastructure and assets in outer space."[14] Additionally, the NSS states that: "Intelligence—and how we use it—is our first line of defense against terrorists and the threat posed by hostile states."[15] This statement, coupled with requirements in the NSHS, unmistakably establishes the need for unity of effort and reinforces the requirement that: "[I]ntelligence must be appropriately integrated with our defense and law enforcement systems…to strengthen intelligence warning and analysis to provide integrated threat assessments for national and homeland security."[16] Accomplishing intelligence fusion and sharing will require unprecedented cooperation and trust within the federal government. Likewise, the requirement for intelligence sharing will test the relationship between the DoD and DHS.

The NSS provides for the use of military capabilities to defeat the threat of terrorism and to support homeland security. In doing so, it establishes a tenuous link between the DHS and the recently

established combatant command, U.S. Northern Command (USNORTHCOM).[17] However, the position shared by DoD and that of Secretary Tom Ridge, the first Secretary of Homeland Security, is that the DHS will not have command or control over USNORTHCOM, but will work through DoD for military support.[18]

The mutually supporting nature of the NSS and the NSHS is reflected in the following subordinate national strategies: the 2001 Quadrennial Defense Review, the National Strategy to Combat Weapons of Mass Destruction, the National Strategy for Combating Terrorism, the National Strategy for Securing Cyberspace, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Drug Control Strategy, and the National Military Strategy.[19] Collectively, these strategies represent the underpinnings of America's strategic defense. Not insignificantly, these strategies, with their increased emphasis on improving homeland security, have begun to blur the traditional distinctions between military and law enforcement actions and roles. An example of this blurring was the deployment of National Guard soldiers into airports and on the nation's borders in the days, weeks, and months following the September 11 attack. The purpose of these deployments was to bolster traditional federal, state, and local law enforcement capabilities to identify and prevent follow-on terrorist attacks. Additional examples include the linking of civilian air traffic control systems with those of the North American Air Defense Command to provide increased warning of potential air threats, and the continued support of DoD's Joint Task Force 6 to the U.S. Customs and Border Patrol to prevent illegal entry of personnel and drugs along the southern border. These examples, coupled with requirements yet to be defined, increasingly challenge DoD as it strives to balance its warfighting requirements with those of supporting homeland security. Defining the relationship between the DoD and the DHS is essential to seeking this balance and represents the formation of the critical requirement that directly supports homeland security as a critical capability.

THE CRITICAL REQUIREMENT: THE RELATIONSHIP BETWEEN THE DEPARTMENT OF DEFENSE AND DEPARTMENT OF HOMELAND SECURITY

An effective, cooperative relationship between the DoD and the DHS is a critical requirement to the securing of the homeland; an ineffective relationship would present a critical vulnerability to the nation's security. Therefore, a commitment to achieving a unity of effort is fundamental in defining this relationship. Interagency disputes and "turf battles" are dysfunctional hallmarks of the federal bureaucracy, especially when funding, prestige, and political influence are at stake. Yet, executing an effective homeland security strategy relies on clear divisions of responsibility, adaptive and flexible supported and supporting relationships, and the sharing of information and intelligence to create a common operating picture among the departments. The objective, or "end," of this strategic relationship is the protection of the American homeland, its people, and the national way of life. The "ways" include cooperative actions across a spectrum of issues, both from a "vertical" perspective by conducting interagency coordination through either the National Security Council (NSC) or Homeland Security Council (HSC) and from a "horizontal" perspective through direct coordination and bilateral cooperation among departments. The "means" include funding and mutually accepted boundaries, especially regarding "dual-use" items, that enhance homeland security.[20] In essence, a functional and effective bridge between the DoD and the DHS depends on breaking new bureaucratic ground to achieve this essential unity of effort.

Creating requirements, whether in legislation or through national strategies, for these departments to coordinate and execute is easier said then done. Forging an effective working relationship to achieve national and departmental objectives will create some interdepartmental friction. However, given the current strategic environment—highlighted by the continuing global war on terrorism, the war with Iraq (Operation IRAQI FREEDOM), concerns over North Korea's nuclear intentions, and a struggling national economy—reducing this friction is critical to addressing

potential critical vulnerabilities. Catastrophic consequences will result from departmental and interagency friction, if it produces excessive parochialism or procrastination.

The DoD and the DHS (once operational) must create organizational mechanisms to coordinate their respective efforts to implement requirements of both national strategies. DoD, by virtue of its traditional mission, organization, and resources, has its own perspective, influenced by its organizational culture, on how to support these strategies. The DHS, as a new and evolving organization, will need to define and create its own institutional perspectives, influenced by its emerging organizational culture. Its overarching mission will define this perspective and how it absorbs and integrates its 22 existing functional organizations, their individual organizational cultures, and institutional biases to form a cohesive department. While no small task, the DHS has an opportunity to bring focus to previously disparate homeland security efforts, create a distinctive organizational culture, and forge a rejuvenated sense of cooperative relationships within the federal bureaucracy. The emerging relationship between these two departments can ensure security of the homeland and protection of the nation's strategic center of gravity.

An assessment of the evolving relationship between these two departments suggests three critical vulnerabilities: (1) use of military forces; (2) intelligence sharing; and (3) funding for homeland security requirements. Each requires immediate attention. A failure to address these potential critical vulnerabilities would leave the nation even more vulnerable to attack.

Use of Military Forces.

As previously mentioned, the increased blurring of military and law enforcement functions poses significant challenges to the DoD and its emerging relationship to the DHS. Though the DHS does not have the investigative authority vested in the Department of Justice for broader law enforcement activities, it does have responsibility for border, immigration, and transportation security, which confers

its own specific law enforcement authority. To execute these requirements, it is likely that the DHS may seek military assets, provided either by the National Guard (in a federalized or state active-duty status) or active duty forces, in support functions closely resembling traditional law enforcement activities.

Section 876 of the HSA 2002 strictly prohibits the DHS from directing or controlling military activities. That section states:

> Nothing in this Act shall confer upon the Secretary [of Homeland Security] any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this act limit the existing authority of DoD or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activity."[21]

Added at the specific request of DoD, this stipulation ensures that direct control of military assets remains with the Secretary of Defense in accordance with Title 10, Unites States Code. Military assets include active duty forces of all four services, their National Guard and Reserve component forces, and supporting DoD agencies. There is one exception—the U.S. Coast Guard.

In accordance with the HSA 2002, the U.S. Coast Guard represents an exception to the DHS's control of a military-type organization. The Coast Guard, a subordinate agency of the DHS as of March 1, 2003, has a military character and culture with a unique mission and a law enforcement capability. On a daily basis, the Coast Guard is responsive and subordinate to the DHS; yet, in time of declared war or if directed by the President, the Coast Guard becomes part of the Department of the Navy under DoD. On a daily basis, DoD relies on the Coast Guard to conduct homeland coastal protection and maritime defense under the control of the DHS. Yet, the Coast Guard represents a unique capability desired by geographical combatant commanders in support of their wartime missions. The recent deployment of eight Coast Guard vessels to the U.S Central Command's Area of Responsibility in support of the war on terrorism and current military action against Iraq, places immediate pressure on the DoD and the DHS to address potential critical vulnerabilities cooperatively.

Whereas the DHS cannot direct nor control military forces in conduct of "homeland defense," under the previously described "extraordinary circumstances" it can request and receive military assets to respond to either "emergency circumstances" or "limited scope circumstances." Similarly, DoD provides military assistance to civil authorities in accordance with DoD Directives 3205 series,[22] and in consonance with the restrictions of the Posse Comitatus Act of 1878.[23] Section 886 of the HSA 2002 affirms the continued restrictions on the use of military forces as a *posse comitatus* to execute the laws of the United States, unless directed by the President to restore domestic order resulting from either an insurrection or as a consequence of an attack by a weapon of mass destruction. An insurrection or an attack by a weapon of mass destruction/effect represents the previously defined "extraordinary" circumstance. DoD, by direction of the President, may become the lead federal agency in stabilizing such a crisis. All other federal agencies employed, including the DHS, would be operating in a supporting role. In this extraordinary circumstance, the Secretary of Defense would assume control of operations based on the restriction that the HSA 2002 imposes on the Secretary of Homeland Security. DoD would remain the lead federal agency only long enough to bring stability to the situation, transferring lead agency responsibility to either the DHS or some other agency, as directed by the President.

While providing traditional military assistance to civil authorities for emergency or limited scope operations, DoD places military assets under the operational direction of a lead federal agency. Consolidating the Federal Emergency Management Agency, the U.S. Border Patrol, the U.S. Customs Service, and the Immigration and Naturalization Services under the DHS casts a wide net across federal agencies which traditionally seek DoD assistance. Respecting the legalities on use of federal military assets—specified in the Posse Comitatus Act, the Stafford Act[24] and the Economy Act[25]—the DHS must centrally generate requests for DoD assistance. Developing this centralized process presents challenges to the DHS, given the experiences each subordinate activity brings with it upon consolidation. A formal memorandum of agreement between the Secretaries of Defense and Homeland Security should establish the broad guidelines for the types of support required, the channels

through which to request support, and metrics for determining the degree and duration of support. Such arrangements provide a common point of reference for both departments, increasing responsiveness and reducing potential friction created by the "fog" normally associated with crisis or catastrophic events.

A common error of federal agencies in seeking DoD support for civil authorities has been undue specificity in their requests for certain types of equipment and manpower. Such specificity frequently leads to delayed response or unnecessary negotiations to clarify actual requirements. The DHS should generalize the tasks or missions and thus permit DoD the latitude to conduct mission analysis and determine troops/equipment-to-task requirements.

Processing requests for military assistance to civil authorities follows a well-defined path within DoD channels. DoD Directive 3025.15 articulates this process.[26] However, the execution of those requests, at times, entails a cumbersome command and control process between the DoD and the supported federal agency. Two actions by the DoD will streamline the support process: first, the activation of USNORTHCOM, as the Department's operational command for supporting homeland security requirements; and second, Congress's approval of the Department's request for an Assistant Secretary of Defense for Homeland Defense. This new assistant secretary, as a senior civilian political appointee, will provide policy direction, coordination and oversight of all departmental efforts related to homeland security.

Within the hierarchy of DoD, this new assistant secretary is subordinate to the Under Secretary of Defense for Policy. This subordination should not, however, prevent the new assistant secretary from coordinating either internally to DoD (including with USNORTHCOM); or externally to DoD, with respect to the DHS. In fact, this assistant secretary should have a statutory arrangement with USNORTHCOM similar to that which the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict has with U.S. Special Operations Command.[27] Such an arrangement would permit a greater degree of civilian oversight and support. Furthermore, the DoD and the DHS should establish direct links between the Assistant Secretary of Defense for Homeland Defense and the Under Secretaries for Border and Transportation Security

and for Emergency Preparedness and Response. Forging these links, despite the disparity in the federal hierarchical "rank" structure, would create an unambiguous formal connection between the departments. This formal connection would become the foundation for bilateral actions and interagency coordination conducted with either the NSC or the HSC. It also would demonstrate that the relationship between the DoD and the DHS represents a critical requirement for the security of the U.S. homeland.

Within the context of this emerging relationship, a potential source of friction exists over determining whether the DHS should coordinate directly its support requests with USNORTHCOM. Based on the preceding discussion, the simple response should be "no." Currently, Secretary Tom Ridge agrees that DoD should retain control over USNORTHCOM's actions (see endnote 17). However, it is essential that a common perspective and channels of communications exist among these organizations. By exchanging liaisons officers, the DHS, the DoD, and USNORTHCOM would facilitate coordination and understanding of departmental capabilities, limitations, and needs. The presence of liaison officers would also aid in identifying and resolving contentious issues before they become critical vulnerabilities.

In sum, abiding by the legal constraints on the use and control of military assets, developing well-thought-out memoranda of agreement that are flexible and adaptive to current and future needs, and exchanging liaison officers between the DHS and DoD, including USNORTHCOM, would represent significant steps towards effective interdepartmental cooperation and reduction of a critical vulnerability. These recommended steps also serve as a foundation for addressing the next two potential critical vulnerabilities.

Intelligence Sharing.

Intelligence is the bedrock for successful anticipation and prevention of future terrorist attacks. It is neither a stand-alone activity nor the domain of any single federal agency. Information acquired from multiple sources—local, state, national, foreign, and

law enforcement—must be analyzed, fused, and translated into predictive intelligence products to permit specific actions that prevent future terrorist attacks. The essential component in this cycle is the sharing of both raw information and refined intelligence products. This presents an immediate requirement for both the DoD and the DHS to establish procedures to affect this sharing. These procedures must satisfy statutory requirements, national strategies, and the organizational interconnectivity of purposes of both departments. Getting these procedures right requires a priority of effort and a willingness to break from institutional prejudices.

DoD supports numerous organic intelligence activities—the National Security Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, and individual Service Intelligence organizations. The Department both acquires and exploits intelligence, supporting its wartime missions and counterintelligence requirements. In the current strategic environment, this intelligence not only supports on-going and future military operations, but also helps identify and prevent terrorist attacks within the homeland. The challenge within the intelligence community, and especially for DoD, is to determine "what to share" and "how to share." Failure to get this right would create a clear and indisputable critical vulnerability.

Section 201 of the HSA 2002, requires all federal agencies to provide information and intelligence products to the DHS for analysis in order to: "(a) identify and assess the nature and scope of terrorist threats to the homeland; (b) detect and identify threats of terrorism against the United States; and (c) understand such threats in light of actual and potential vulnerabilities of the homeland." Historically, intelligence sharing among federal agencies has been weak; it was also a significant factor in the failure to identify and prevent the September 11 terrorist attacks.

Sharing intelligence raises three key issues: first, DoD must determine what information is relevant to homeland security, as opposed to other nondomestic and foreign national defense issues; second, both departments must address the current intelligence classification system, which hinders release of critical predictive intelligence products; and third, both departments must establish organizational linkages to support the intelligence sharing

process.[28]

Determining the information and intelligence requirements that support the DHS's mission will be a continuous process. The NSHS and the statutory requirements of the HSA 2002 provide some direction, but the specifics require continual refinement according to current and anticipated demands. Without further guidance, as the DHS becomes operational, it is possible that it will possess less information than it deems essential for mission requirements. Without more specific guidance, DoD will most likely only share intelligence it deems pertinent to homeland security (as opposed to intelligence with broader national security implications), citing sensitivity of its intelligence and the need for operational security. The need to protect the methods and sources used to collect and corroborate the data often restricts the distribution of intelligence products, even for legitimate reasons. The passing of intelligence products to a new and untested agency will require significant safeguards to protect the information, methods and sources from which the information was acquired.[29]

The expectation that intelligence, whether from DoD or other agencies, will be readily distributed is at best, wishful thinking. This is not to imply a deliberate effort by any agency or department to circumvent the law. It is, however, an acknowledgement that intradepartmental culture influences interdepartmental behavior and contributes to distrust among agencies. This distrust, and its intradepartmental cultural roots, represents an obstacle that departmental leaders must reduce. For the Central Intelligence Agency and the intelligence agencies within DoD, the inadvertent release of sensitive information may jeopardize current or future operations. While this may represent a reason not to share or to limit the extent of information provided, protecting the U.S. homeland, while combating terrorism, is a vital security interest and argues for providing the DHS with such information.

To facilitate this sharing process, both departments should jointly determine the types of information required—including both raw and refined products—and from which collection platforms they are to come. By defining parameters—which may include targeting specific individuals and organizations outside the borders of the nation and placing a priority of collection on those requirements—

DoD can integrate requirements within its own collection plan, thereby reducing duplicity and stress on the system. In the long run, the ability of the two departments to agree on parameters and establish their own coordination system is much preferred to having Congress legislate such specifics. The use of a common secure information sharing network, analysts sensitized to both national and homeland security requirements, and the exchange of liaison officers is critical to the rapid transfer and synthesis of information and intelligence.

Inherent in the information determination and sharing process is the need to address the current classification system for relevance to homeland security. The unauthorized disclosure of national intelligence products could cause severe and potentially irreparable harm to the nation. This places both the DoD and the DHS in a paradoxical situation. Predictive intelligence, essential to implementing defensive or preventive measures, potentially may not be distributed due its security classification and/or the lack of security clearance of the intended recipients. Yet, one of the statutory purposes of the DHS is to assess intelligence and provide warning to national, state, and local agencies. To meet this requirement, the DHS must develop the means to declassify or sanitize intelligence effectively, making it both available and useful to those at the appropriate implementing levels. Establishing a homeland security classification system is critical to providing warning and vulnerability assessments to the appropriate federal, state, or local officials.

The establishment of a homeland security classification system for information and intelligence, discussed shortly after the stand-up of the Office of Homeland Security in October 2001, ended without a viable system.[30] Perhaps it is time to reassess this idea. The necessity of passing intelligence information through the DHS network is essential. Beyond the current Homeland Security Advisory System, the DHS must be able to use the contents of these predictive products, regardless of their classification, to initiate more specific preventive homeland security measures. The cooperation of DoD (and other affected agencies such as the CIA), must result in a system which jointly sanitizes and assigns an appropriate homeland security classification code to pertinent classified intelligence.

Such a system would provide both a disciplined approach to the amount and type of intelligence distributed, keyed to a "need-to-know" requirement, and ensure protection of the most sensitive aspects of intelligence from unauthorized disclosure. The alternative is to continue to rely upon the current classification system. But that would require thousands of federal, state, and local individuals who support homeland security requirements, to undergo security investigations in order to meet current requirements. The number of personnel who might have a homeland security "need-to-know" would overwhelm an already struggling Defense Investigative Service. However, by establishing a homeland security specific reclassification process and coordinating product contents with the DoD, the DHS could assess threats, determine vulnerabilities, and provide predicted targeted warning of potential attacks to the appropriate level. The specifics of such a system and the details of the appropriate translation of classifications are beyond the scope of this chapter. Yet, the interagency coordination process must address the concept of a homeland security specific classification system. The NSC and the HSC should both approve the resulting intelligence sharing methodology. From a strategic perspective, such an effort is an essential step in enabling the DoD and the DHS to support both statutory and strategy driven requirements cooperatively, while simultaneously conducting their independent mission requirements related to national and homeland defense.

Coordinating the requirements of determining what information to share and how to address the classification of the information should rest on specific organizational offices within each department. The HSA 2002 establishes an Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection, whose responsibilities include acquisition and analysis of intelligence and comprehensive vulnerability assessment. Additionally, the National Defense Authorization Act for Fiscal Year 2003 authorized DoD's request for a new under secretary position: the Under Secretary of Defense for Intelligence. Though this act requires that the DoD define the mission and organizational structure of this new office to Congress, including the relationship with various internal departmental offices and the Departments' intelligence gathering activities, it does not address the need for a relationship with the DHS. This oversight is

unquestionably a strategic error, but one easily corrected. The DoD, as part of its response to the Congressional requirement, should address the implied, but strategically essential connection, between the two departments' respective under secretaries.[31] Codifying this relationship, based on the requirement to share intelligence for homeland security, the DoD and the DHS can meet statutory and strategy driven national and homeland security obligations and create the conditions to eliminate a critical vulnerability. The need for this codification further demonstrates that the relationship between the DoD and DHS is a critical requirement for effective homeland security. It also provides a template for addressing the third potential critical vulnerability.

Funding of Homeland Security Related Requirements.

Having budget authority conveys significant bureaucratic power within the federal government. In Fiscal Year 2004, the DoD projects a budget of over $380 billion and the DHS projects approximately $36.2 billion. Until recently, federal budgeting has been both a finite and a "zero-sum" process; in essence, for every increase in one department's budget, other departments or agencies generally experience a decrement. The funding of both departments for homeland security requirements and corresponding technological research and development will create friction, as each department commits resources to support its specific programs. Despite the Bush administration's willingness to engage in deficit spending to wage the war on terrorism, funding for homeland security and national security requirements remains finite. Friction, created by bureaucratic maneuvering to increase departmental budgets, is a critical vulnerability that the departments must avoid.

The broad objectives and numerous ambitious programs contained within the NSHS, and supporting statements within the NSS, beg the obvious concern of how to fund these programs, while simultaneously maintaining funding for other critical federal programs, including national defense. From a macro-perspective, this is not entirely a specific concern of the DoD. However, a closer

examination of the interrelations among requirements indicates that the DoD and the DHS must address such specific areas as: (1) transfer of technology and equipment that could support homeland security; (2) improving first responder capabilities: and (3) reimbursement for supporting DHS specific missions (i.e., military assistance to civil authorities). The first two areas, though implied in the NSHS, are specifically addressed in the National Defense Authorization Act of Fiscal Year 2003. The Stafford and Economy Acts—the legal basis by which one federal department provides support for another and how they are reimbursed—addresses the third area. The DoD has significant experience under both acts of providing support to and receiving reimbursement from various federal agencies for military assistance to civil authorities. However, the DHS's developing operational structure and lack of institutional processes for addressing reimbursement issues, notwithstanding the experiences of its subordinate agencies before their transfer to the department, may create friction with the DoD. The rigorous application of the Stafford and Economy Acts and development of memoranda of agreements will reduce or eliminate such friction. Under no circumstances should reimbursement issues affect execution of vital homeland security missions.

Some of the technologies being developed for improving soldier and unit capabilities on the battlefield have direct application—i.e., dual-use—in homeland security. These DoD funded capabilities overlap with many of the DHS responsibilities. Examples include chemical and biological identification technology, protective equipment, decontamination equipment, and common communications devices. DoD by necessity is at or near the forefront of many of these technologies. For DoD, these technologies and capabilities are essential to support and conduct combat operations in environments where weapons of mass effects may exist. Although the transfer of these and other related technologies and capabilities would benefit the DHS and the first responder community, the DoD should not have to cede complete control of this effort or unilaterally fund this research and development without a cost-sharing agreement. Though the DHS has a statutory obligation to invest in, develop, and procure common equipment to support first responder capabilities, the DoD must also conduct research, development, and

acquisition of similar or identical capabilities to protect soldiers on the battlefield. Determining exact costs and shared responsibilities is beyond the scope of this chapter. However, the DoD and the DHS should establish a specific relationship to address these areas, assess the associated financial costs, determine if efficiencies are possible, and coordinate essential research, development and acquisition requirements and strategy.

To facilitate this recommendation, the under secretaries from each department whose primary duties include responsibility for oversight of technology development and acquisition, should establish a formal relationship. For the DHS, this responsibility falls to the Under Secretary for Science and Technology, and for the DoD, it falls to the Under Secretary for Acquisition, Technology, and Logistics. It is likely that at least two other subordinate offices within the DoD need to be involved in coordinating these activities, the new Assistant Secretary of Defense for Homeland Defense and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

As with the sharing of intelligence and establishing boundaries for the use of military assets, the establishment of direct organizational links between these officials can preempt potential problems. Though not specifically required by strategy or statute, the formal articulation of these relationships in memoranda of agreement can ensure a unity of effort. However, the specifics of funding may become a significant point of friction between departments and could ultimately require either a presidential directive (issued through the Office of Management and Budget) or Congressional intervention, as part of the normal budget process. Solving funding issues either bilaterally or through the interagency process is in the national interest, as well as each agency's interests. Failure to resolve these issues may foster continuous friction between the departments and create a critical vulnerability. This vulnerability could manifest itself in a lack of first responder or soldier preparedness to confront the consequences of a future terrorist attack. The results would transcend bureaucratic politics and directly affect the lives of soldiers and first responders, particularly if use of weapons of mass destruction/mass effects are involved.

The DoD and DHS must cooperatively address the potential critical vulnerabilities presented by the use of military force, the sharing of intelligence, and the funding of homeland security requirements. Failure to do so, either by adopting or modifying the recommendations presented, opens the nation to attack. If bilateral agreements cannot resolve these critical vulnerabilities, the departments must address the vulnerability either to the NSC or the HSC for resolution.

RESOLVING CRITICAL VULNERABILITIES: THE NATIONAL SECURITY COUNCIL VS. THE HOMELAND SECURITY COUNCIL

"Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government."[32] This statement reflects the fundamental aspect of the federal government's responsibility and underscores the DoD and the DHS's relationship as a critical requirement for homeland security. It also provides an overarching means for addressing current and future critical vulnerabilities. Both departments undoubtedly will endeavor to do what is best for the nation; however, each department will have differing approaches to fulfilling their portion of this commitment. Their approaches may, as an unintended consequence, create potential vulnerabilities.

The creation of the DHS will generate friction within the federal bureaucracy. While some friction can be healthy to organizational development and interorganizational relations (e.g., by ensuring constant attention to organizational mission objectives), friction can also, in the Clausewitizian sense, lead to less positive outcomes. Identifying and addressing potential friction points facilitates both departments' prospects for mission successes, creates conditions to eliminate critical vulnerabilities, and fosters a seamless cooperative effort to protect the nation's homeland and national centers of gravity.

The NSC and HSC are the two presidential decision forums for coordinating interagency actions and developing national

policy. They also represent the strategic "way" to reduce the critical vulnerabilities described in this chapter. Each Council has its own purpose, but their scope of concerns are beginning to overlap given the increasing interrelatedness of national and homeland security issues.

The National Security Act of 1947 established the NSC with the stated purpose to:

> (a) . . . advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.[33]

For over 50 years, this council has served as the primary conduit of integration and interagency coordination affecting domestic and foreign policy related to national security, including domestic security considerations within the United States. The council's organizational structure is flexible, reflecting each president's policy and decision making style. The current administration has structured its council around regional and functional policy coordinating committees to provide recommendation to a Deputy's Committee, which in turn refines the issues for decision by the Principals Committee. Inherent in this deliberative staffing process is the need to assess risks to the national security and report or make recommendations to the President accordingly.

The HSC, established by Presidential Executive Order 13228 on October 8, 2001, and provided statutory recognition in the HSA 2002, parallels the function and structures of the NSC, but with a narrowly defined focus on homeland security and the prevention of terrorism. The HSC:

> . . . shall be responsible for advising and assisting the President with respect to all aspects of homeland security. The Council shall serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies. [34]

The NSC has four statutory members: the President, Vice President, Secretary of Defense, and Secretary of State; the Chairman

of the Joint Chiefs of Staff is the council's statutory military advisor. By contrast, the HSC has five statutory members: the President, Vice President, Secretary of Defense, Attorney General, and Secretary of Homeland Security; it does not have a statutory military advisor. The omission of two key personnel, the Secretary of State and Chairman of the Joint Chiefs of Staff, significantly narrows the focus of the HSC.[35] The Secretary of State attends meetings only if there are matters pertaining to his area of responsibility and the Chairman of the Joint Chiefs (CJCS), initially not permitted to attend, eventually received a standing invitation to all meetings.

In the aftermath of the September 11 terrorist attacks, the creation of the HSC initially frustrated DoD, vis-à-vis the traditional role of the NSS. The department's frustrations resulted from the HSC's "growing pains" as it struggled to become operational in the midst of a national crisis. These initial growing pains revealed three HSC shortfalls: (1) haphazard interagency coordination processes; (2) lack of refined internal operating procedures; and (3) couching national issues under the rubric of "homeland security" without a clear definition of homeland security. The omission of military representation, specifically the CJCS, as either a formal member or advisor to the HSC, further frustrated the department. This lack of formal military representation denied relevant military advice to the President and the Secretary of Defense during the initial HSC Principals Committee meetings. This military advice was also lacking in the numerous deliberations in policy coordinating committees and the deputy's committee meetings. Currently, the CJCS, or his designated representative, has a standing invitation to all HSC meetings, including deputy and policy coordinating committee meetings. However, there has been no amendment to the executive order or the HSA 2002 to reflect this arrangement. This organizational flaw is significant; it stands in stark contrast to the NSC where the CJCS is the statutory principal military advisor to the council. The statutory omission of the CJCS and the Secretary of State from HSC deliberations, both critical advisors to the president, suppresses consideration of broader national policy implications on homeland security decisions.

It is important to note, that in accordance with Section 102 (d) of HSA 2002, "the Secretary [of Homeland Security] may, subject to

the direction of the President, attend and participate in meetings of the National Security Council." On the other hand, it ensures that homeland security equities are represented during NSC discussions and formulation of national policy. However, simultaneous memberships by the Secretaries of Defense and Homeland Security on both councils, creates inevitable friction in determining how and where to address matters related to homeland security within the interagency process.

The creation of a separate interagency forum for addressing homeland security issues may at first seem appropriate, particularly given the failure of U.S. strategic defenses to detect, identify, and prevent the attacks of September 11, 2001. However, the NSC coordinated and responded to all national security related issues, as defined by Presidential Executive Order 12656 (November 18, 1988), prior to the establishment of the HSC. One could reasonably interpret these issues, termed "national security emergencies," to include terrorism. A national security emergency, as defined by Executive Order 12656 is:

> . . . any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States. Policy for national security emergency preparedness shall be established by the President. Pursuant to the President's direction, the National Security Council shall be responsible for developing and administering such policy.[36]

The advantage of addressing all national security related matters within the NSC, as defined by its the charter and within the parameters of the executive order above, ensures an integration of foreign and domestic considerations. Today this is especially pertinent, given the increasing effects of globalization. Few actions, whether domestic or foreign, occur in isolation. Actions or decisions made in support of homeland security have both direct and indirect impact on foreign affairs and vice versa. The creation of a parallel structure for homeland security has potential for bifurcating both the decision process and consideration of potential consequences. At the very least, maintaining two distinct decision forums requires narrowly defined, homeland security specific actions to be separated

from those of a broader national security nature. Given the interconnectivity of the NSS and NSHS, and the need for coordinated efforts by the DoD and the DHS, making these clear distinctions continues to be a difficult process. For DoD, participating at all levels in both councils requires a constant effort to reconcile and balance national security related actions with those of homeland security. This effort will become even more strenuous and essential once the DHS becomes operational. Fortunately, to date, both councils appear to be working in tandem; however, it is too early to assess the long-term implications of maintaining parallel forums.

Within the context of these parallel forums, selecting the specific forum for interagency coordination has implications for each department. For DoD, the NSC offers the better strategic forum for obtaining balanced decisions affecting its domestic and foreign security commitments. By contrast, the DHS would most likely prefer the HSC's primary narrow domestic focus, with secondary considerations for the broader foreign policy implications.

Citing specific unclassified examples explaining why the DoD should prefer to take issues to the NSC rather than the HSC is difficult, given the sensitivity of the specific actions and security concerns of both forums. However, consider the following scenario:

DoD directs through its annual Contingency Planning Guidance that each Geographic and Functional Combat Commander, using the Deliberate Planning Process, develop specific contingency plans, operations plans or functional plans for their specific area of responsibility. Many of these plans require interagency coordination to ensure national supportability. The specifics of the requested interagency support are defined in Annex V, entitled Interagency Coordination, of each plan.[37] In compliance with the Contingency Planning Guidance, U.S. Northern Command, as well as U.S. Pacific Command and U.S. Southern Command, both geographic combatant commanders with responsibilities for supporting homeland security, must develop individual plans with supporting Annex V's. Coordinating these annexes requires the DoD to submit them to either the NSC or the HSC. Logic would dictate submission to the HSC; however, the DoD is unlikely to do so. Though the focus of each plan is to support homeland security, there are other broader national security implications to be considered: specifically,

the strategic impacts of designating forces (air, land and maritime, including requests for Coast Guard assets) to respond to either "extraordinary" or "emergency" circumstance requirements, while simultaneously conducting or preparing to execute other contingency operations in support of the NSS. This does not imply that the domestic aspects of these annexes should be ignored; rather, these annexes should be coordinated with consideration to foreign policy concerns by the NSC. By doing so, DoD would obtain an integrated and balanced foreign and domestic assessment to support each combatant commander's needs. Further, since the Secretary of Homeland Security, is an invited member of the NSC, he would be expected to use the Office of Homeland Security to coordinate review and comments on these annexes. He would submit this review, with its specific emphasis on homeland security, as his response to the NSC staff. Using the staffing process of the NSC, DoD insures the most comprehensive review of these annexes. As long as America remains a nation at war, conducting simultaneous offensive and defensive actions, the NSC is the one best forum to conduct interagency coordination given its holistic view of foreign and domestic strategic choices and risks.

Parallel decision forums, with overlapping memberships but distinctly different objectives, present both departments, and the interagency in general, with a challenging problem of balancing domestic needs with on-going foreign commitments. The HSC, after just over 18 months of operations, is still maturing. It has, however, made significant strides and has become, by force of the President's directive, an organization that is gaining respect within the federal bureaucracy. However, in the months since Congressional confirmation of Secretary for Homeland Security Tom Ridge, the President has not appointed a new Assistant to the President for Homeland Security. Absent such an advisor to direct the Office of Homeland Security and the day-to-day actions of the HSC, it remains to be seen whether this council will continue as a separate organization. It is likely, given the increased blurring of national and homeland security matters, the inclusion of the Secretary for Homeland Security on the NSC (at the President's determination), and the exclusion of the Secretary of State from the HSC (unless invited), that the Office of Homeland Security and the functions of

the HSC may soon become subordinate to the NSC.

In the interim, determining how and where to address contentious issues will remain a matter of deciding relevance: Is the issue of broader relevance to national security or is it more focused on homeland security and preventing terrorism? The forum provides the context from which the presidential decision is both debated and rendered. For the DoD, this will require a case-by-case determination; for the DHS, the matter is more clearly defined.

CONCLUSION

> We have seen the problem and it is us![38]

To comply with Secretary Rumsfeld's epigraph at the beginning of this chapter and in seeking to work with the DHS to provide for the nation's defense, the DoD must now put deeds behind words. As the more established and senior partner in this strategic relationship, the DoD must assume greater responsibility for developing an effective relationship with the DHS. In seeking to create this relationship, both departments must acknowledge a harsh reality of organizational culture and behavior: "*We have seen the problem and it is us.*" That is, organizations frequently place obstacles in their own path. However, organizations also have the ability to remove those obstacles, and this is clearly applicable to the critical vulnerabilities identified within this chapter. These vulnerabilities are not insurmountable. The vulnerabilities presented can be resolved by "us"—that is, the leadership of both the DoD and the DHS.

Homeland security, as a critical capability, offers fundamental protection to the nation. It represents a cohesive strategic defense permitting the nation to execute its national strategies while simultaneously prosecuting the war on terrorism. Further, there is little doubt that an effective relationship between the DoD and the DHS represents a critical requirement that enables homeland security as a critical capability. More than any two other departments within the federal government, the DHS (charged by law and the NSHS to protect the nation's homeland from terrorism) and the DoD (charged by law and the NSS to not only defend this nation but to

concurrently fight and win the nation's wars), must achieve a unity of effort. Anything less creates critical vulnerabilities and imperils the nation's center of gravity.

The emerging relationship between the DoD and the DHS requires constant efforts to identify and defuse potential bureaucratic tensions. DoD is still defining its roles, missions, and relationships relative to increased homeland security requirements, as well as assessing how it must interact with the DHS. This chapter has sought to promote a greater understanding between departments and to help inform the development of this relationship. The recommendations offered may or may not reflect any ultimate decisions. The dynamics of the current strategic environment, including DoD's transformation efforts and the organizational challenges of standing-up the DHS, all serve to influence the final outcome.

Finally, a strong, cooperative relationship between the DoD and the DHS—focusing on the protection of the American homeland, while avoiding the types of rivalries that have traditionally encumbered the bureaucratic process—will ensure the long-term security of the nation. As President Bush declared on September, 2001, " The conflict was begun on the timing and terms of others. It will end in a way, and an hour, of our choosing."[39]

When this war on terrorism does end, it is certain that this new focus on homeland security will endure, both as a permanent condition for the nation and as a permanent mission for both the DoD and the DHS. Properly nurtured, the resulting relationship will ensure that, no matter who the enemy is or how he attempts to attack this nation, there will be fewer critical vulnerabilities to be exploited in the nation's national security armor.

ENDNOTES - CHAPTER 10

1. George W. Bush, "Address to the Joint Session of Congress and the American People," September 20, 2001; available from *http://www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html*, Internet, accessed September 22, 2002.

2. Department of Defense, "Joint Publication 5-00.1 Joint Doctrine for Campaign Planning," Washington, DC: Department of Defense, 25 January 2002,

p. II-6. Center of Gravity: "Those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight." (Note: Our national will is clearly a source of our national power and strength in the war on terrorism and, as a strategic center of gravity, must be protected from attack.)

3. *Ibid*., p. II-7. Critical Capability: "Those adversary capabilities that are considered crucial enablers to the adversary's center of gravity to function as such and essential to the accomplishment of the adversary's assumed objective." (Note: though this definition is focused on the analysis of an adversary's capabilities, this concept applies equally to determining our own strategic critical capabilities, requirements and vulnerabilities as critical factors linked to our strategic center of gravity.)

4. *Ibid*., p. II-7. Critical Requirement: "Those essential conditions, resources, and means for a critical capability to be fully operational."

5. *Ibid*., p. II-7. Critical Vulnerability: "Those aspects or components of the adversary's critical capabilities (or components thereof) which are deficient, or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results, disproportionate to the military resources applied."

6. This thought, while not original, has been much debated and discussed in various journals and professional forums. It is not possible to attribute this comment to a specific source or sources.

7. George W. Bush, "The National Strategy for Homeland Security," Washington, DC: The White House, July 2002, Introduction.

8. *Ibid*., p. vii.

9. *Ibid*., p. viii.

10. This assessment is based on the public statements in various news media and congressional debates regarding the proposed budget for the DHS and the estimate of the number of federal employees affected by the merger of the 22 specified agencies. The assessment of the DHS budget in comparison to other federal agencies is based on the President's FY2004 budget submitted by the Office of Management and Budget; available from: *http://www.whitehouse.gov/omb/budget/fy2003/pdf/hist.pdf*, Internet, accessed February 3, 2003.

11. "Homeland Security Act of 2002." Public Law 107-296. sec. 101, p. 8, November 25, 2002.

12. *Ibid*.

13. Donald Rumsfeld, Testimony to House Select Committee on Homeland Security, July 11, 2002, accessed from: *http://www.defenselink.mil/speeches/2002/s20020711-secdef.html*, Internet, accessed September 22, 2002.

14. George W. Bush, "The National Security Strategy for the United States of America," Washington, DC: The White House, September 2002, p. 30.

15. *Ibid*.

16. *Ibid*. (Note: the ability to integrate intelligence is not just a Department of Defense function but will require the coordination of several federal agencies including the CIA.)

17. The National Security Strategy for the United States of America does not specifically identify U.S. Northern Command by name; rather it references "a new unified command" (see page 6). When the National Security Strategy was being drafted, the designation of U.S. Northern Command, as part of Unified Command Plan 2002, was pending Presidential approval.

18. On January 22, 2003, he was sworn in as the first Secretary of the Department of Homeland Security by Vice President Richard Cheney.

19. Each strategy, while focused on a specific aspect of national or homeland security, are all complementary and interconnected to ensure security of the nation. The order presented does not reflect any specific status or hierarchical precedent, rather, date of publication. A brief summation of these supporting strategies follow are:

> "The Quadrennial Defense Review," September 2001. This review, required every four years by Congress, sets the new defense strategy that embraces uncertainty and contends with surprise. This review is premised on the idea that to be effective abroad, America must be safe at home. The defense strategy acknowledges a new emphasis on the unique operational demands associated with the defense of the United States and restores the defense of the United States as the Department's primary mission. The strategy is therefore built around four key goals that will guide the development of U.S. forces and capabilities, their deployment and use: (1) Assuring allies and friends of the United States' steadiness of purpose and its capability to fulfill its security commitments; (2) Dissuading adversaries from undertaking programs or operations that could threaten U.S. interests or those of our allies and friends; (3) Deterring aggression and coercion by deploying forward the capacity to swiftly defeat attacks and impose severe penalties for aggression on an adversary's military capability

and supporting infrastructure; and (4) Decisively defeating any adversary if deterrence fails. A central objective of the review was to shift the basis of defense planning from a "threat-based" model that has dominated thinking in the past to a "capabilities-based" model for the future. This capabilities-based model focuses more on how an adversary might fight rather than specifically whom the adversary might be or where a war might occur.

"The National Strategy to Combat Weapons of Mass Destruction," December 2002. An effective strategy for countering WMD, including their use and further proliferation, is an integral component of the National Security Strategy of the United States of America. As with the war on terrorism, the National Strategy for Homeland Security, and the new concept of defense, the U.S. approach to combat WMD represents a fundamental change from the past. The three pillars of this national strategy are: (1) Counter-proliferation to Combat WMD Use; (2) Strengthened Nonproliferation to Combat WMD Proliferation; and (3) Consequence Management to Respond to WMD Use. Four cross cutting enablers for these pillars are: (1) intelligence collection and analysis on WMD, delivery systems, and related technologies; (2) research and development to improve our ability to respond to evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile states and terrorists.

"The National Strategy for Combating Terrorism," February 2003. This strategy outlines efforts in the nation's war against global terror and complements both the National Security Strategy and the National Strategies for Homeland Security. The strategy establishes critical goals for strengthening America's security against the threats of the 21st century and describes efforts to disrupt and identify potential terrorist attacks before they take place.

"The National Strategy for Securing Cyberspace," February 2003. This strategy aims to ensure that Internet disruptions are infrequent, of minimal duration, manageable, and cause the least damage possible. The plan depends on coordinated effort from federal, state and local governments, the private sector, and citizens. The objective is to reduce the nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them.

"The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets," February 2003. This strategy

includes provisions for protecting the roads, industrial plants, and energy systems that make up the country's critical infrastructure. In a foreword to the document, President George W. Bush writes that it "provides a unifying structure, defines rules and responsibilities, and identifies major initiatives that will drive our near-term protection priorities." The document outlines what government and the private sector should do to safeguard the country's vital assets. It calls on business sectors to share information on threats while promising federal guidance to help assess the vulnerability of key infrastructure components.

"The National Drug Control Strategy," February 2003. This strategy is intended to reduce the usage of and flow of drugs into this country. It establishes three priorities: (1) stop drug use before it starts; (2) heal America's drug users; and (3) disrupt the drug market. While focusing heavily on demand reduction, the strategy also recognizes the importance of eroding the economic base of the drug trade. Every step that makes the drug trade more dangerous and less profitable for drug dealers is a step toward "breaking" the international and domestic market for illegal drugs. These efforts are complementary to both national security and homeland security strategies.

"The National Military Strategy for the United States of America (Draft)," February 2003. This strategy, informed by the Quadrennial Defense Review, is the Chairman of the Joint Chiefs of Staff's guidance to Service and Combatant Commanders for employing joint military capabilities in support of the requirements of the National Security Strategy. The key pillars of the draft National Military Strategy are: (1) Protect the United States, Allies and Interests; (2) Prevent conflict and surprise attacks; and (3) Prevail against all adversaries. These three pillars horizontally support, through military efforts, the four tenets of the National Security Strategy: Assure, Dissuade, Deter, and Defeat.

20. A "dual-use" item refers to equipment that has application both for military and civilian uses. In this use, it refers to equipment designed to protect soldiers from the effects of weapons of mass destruction and which may also have application for first responders in support of homeland security missions. These items generally include nuclear, biological, and chemical protective equipment (i.e., protective clothing and gas masks, detection and decontamination equipment, and communications equipment). Creating items with dual use capability is cost effective and helps to standardize equipment and protective procedures across the first responder community. Dual use items also enhance interoperability among first responders and the myriad of supporting agencies from local through state

and federal levels.

21. "The Homeland Security Act of 2002," sec. 876, p. 110, November 25, 2002.

22. Department of Defense 3025-series Directives related to providing military assistance and military support to civil authorities for homeland security requirements under emergency or limited scope circumstances are: Department of Defense Directive 3025.1, "Military Support to Civil Authorities (MSCA)," dated January 15,1993; Department of Defense Directive 3025.12, "Military Assistance for Civil Disturbances (MACDIS)," dated February 4, 1994; Department of Defense Directive 3025.13, "Employment of Department of Defense Resources in Support of the United States Secret Service," dated September 13, 1985; Department of Defense Directive 3025.15. "Military Assistance to Civil Authorities," dated February 18, 1997; and Department of Defense Directive 3025.16, "Military Emergency Preparedness Liaison Officer (EPLO) Program," dated December 18, 2000.

23. "Crimes and Criminal Procedure Act." U.S. Code. Title 18, s**ec. 1385.** The Posse Comitatus Act (PCA) states: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws, shall be fined under this title or imprisoned not more than two years or both." (Note: PCA is vague and subject to a wide range of legal interpretations; Congress has modified but never clarified the vagueness of the Act since its passage in 1878. PCA's original legal intent was to prevent local law enforcement officials from pressing federal troops/soldiers into posse service in the post-Reconstructionist South. PCA has consistently, but narrowly, been interpreted to preclude federal military forces from acting as a national police force or enforcing laws without express consent of the President or Congress. By Department of Defense Directive 5525.5 [Department of Defense Cooperation with Civilian Law Enforcement Officials], PCA also applies to the Navy and Marine Corps. PCA does not apply to the Coast Guard, which is both an armed force and a law enforcement agency with commensurate powers. PCA does not apply to the National Guard operating in a state active duty capacity but has been interpreted to apply when in a federalized status.) Available from: *http://www4.law.cornell.edu/uscode/18/1385.html*, Internet, accessed September 22, 2002.

24. "Robert T. Stafford Disaster Relief And Emergency Assistance Act," P.L. 93-288, as amended. The intent of Congress, by this Act, is to provide an orderly and continuing means of assistance by the Federal Government to State and local governments in carrying out their responsibilities to alleviate the suffering and damage which result from such disasters. Federal agencies may be reimbursed for expenditures under this Act from funds appropriated for the purposes of this Act. Any funds received by Federal agencies as reimbursement for services or supplies

furnished under the authority of this Act shall be deposited to the credit of the appropriation or appropriations currently available for such services or supplies. Available from *http://www.ohioema.org/robertt.htm*,Internet, accessed October 1, 2002.

25. "The Economy Act," U.S. Code. Title 31, sec. 1535, permits one agency (requiring agency) to use its appropriations to fund another agency (servicing agency) to supply, render, or obtain by contract supplies or services for the requiring agency. This essentially permits one agency such as Department of Defense to provide support to another federal agency and at the same time request reimbursement for providing such support. Available from: *http://propertydisposal.gsa.gov/ResourceCenter/laws_regs_all/economy/economy.html, Internet,* accessed September 22, 2002.

26. Department of Defense Directive 3025.15, "Military Assistance to Civil Authorities," provides the specific channels, processes, and approval chain for civilian agencies to request federalized military assistance to civil authorities.

27. "The Armed Forces Act." U.S. Code. Title 10, sec 138. This Act provides that:

> The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict . . . shall have as his [Secretary of Defense] principal duty the overall supervision (including oversight of policy and resources) of special operations activities (as defined in section 167(j) of this title) and low intensity conflict activities of the Department of Defense. The Assistant Secretary is the principal civilian adviser to the Secretary of Defense on special operations and low intensity conflict matters and (after the Secretary and Deputy Secretary) is the principal special operations and low intensity conflict official within the senior management of the Department of Defense.

Using this relationship as a template, the ASD for Homeland Defense should be given the same latitude in his relationship with U.S. Northern Command to support DoD's homeland security requirements; available from *http://www4.law.cornell.edu/cgi-bin/empower*, Internet, accessed September 22, 2002.

28. DoD is only one of several intelligence gathering and using agencies that will be required to coordinate and share information with DHS. The FBI and CIA will be the focus of the majority of national and Congressional attention. Yet, DoD, with 80 percent of the federal intelligence budget and the substantial intelligence gathering assets, must work in close collaboration with the CIA to support national security efforts.

29. The concept of the DHS as a "new and untested agency" is not an original thought. Rather, it is one that has appeared in numerous articles addressing the challenges that the new department will face in establishing itself and in developing working relationships with other federal agencies. The concept addresses the relative newness of the organization, its mission, its internal processes, and the need for the majority of its personnel to confront the plethora of issues we now define within the rubric of homeland security.

30. This observation is based on personal experience while assigned as a strategic planner in Homeland Security Division, Joint Staff J-5 (Strategic Plans and Policy Division). The Homeland Security Classification system was discussed at HSC policy coordinating committee and deputies committee meetings. The subject was eventually dismissed as impractical due to the difficulties in sanitizing and reclassifying information for distribution.

31. "The Bob Stump National Defense Authorization Act For Fiscal Year 2003," sec. 137. This Act requires the Secretary of Defense to submit to congress a report on the establishment of the position of Under Secretary of Defense for Intelligence. This report must include the mission, organizational structure, relationships with the Under Secretary of Defense for Acquisition, Technology and Logistics and the Under Secretary of Defense for Policy and each of the intelligence components of the Department of Defense (NAS, DIA, NIMA, and NRO). It does not specify any specific requirement to address a relationship to Department of DHS.

32. Bush, "The National Strategy for Homeland Security," Introduction.

33. "The National Security Act 1947," U.S. Code., sec. 402. Available from *http://www4.law.cornell.edu/uscode/50/402.html*, Internet, accessed September 22, 2002.

34. George W. Bush, Executive Order 13228 of October 8, 2001. "Establishment of the Office of Homeland Security and the Homeland Security Council." Available from: *http://www.fas.org/irp/offdocs/eo/eo-13228.htm*, Internet, accessed September 22, 2002.

35. National Security Act of 1947, sec 101, states:

> The National Security Council is chaired by the President. Its regular attendees (both statutory and non-statutory) are the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Chairman of the Joint Chiefs of Staff is the statutory military advisor to the Council, and the Director of Central Intelligence is the intelligence advisor. The Chief of Staff to the President, Counsel to the President, and the Assistant to the President for Economic Policy are invited to attend

any NSC meeting. The Attorney General and the Director of the Office of Management and Budget are invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies, as well as other senior officials, are invited to attend meetings of the NSC when appropriate.

Presidential Executive Order 13288 states:

> The membership of the Homeland Security Council: President, the Vice President, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Transportation, the Director of the Federal Emergency Management Agency, the Director of the Federal Bureau of Investigation, the Director of Central Intelligence, the Assistant to the President for DHS, and such other officers of the executive branch as the President may from time to time designate. The Chief of Staff, the Chief of Staff to the Vice President, the Assistant to the President for National Security Affairs, the Counsel to the President, and the Director of the Office of Management and Budget also are invited to attend any Council meeting. The Secretary of State, the Secretary of Agriculture, the Secretary of the Interior, the Secretary of Energy, the Secretary of Labor, the Secretary of Commerce, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, the Assistant to the President for Economic Policy, and the Assistant to the President for Domestic Policy shall be invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies and other senior officials shall be invited to attend Council meetings when appropriate.

(Note: Section 901 of The Homeland Security Act of 2002 provides the Homeland Security Council with statutory recognition. The act designates only five members of the council—the President, the Vice President, the Secretary of Homeland Security, the Attorney General, and the Secretary of Defense—but enables the President to name other members as he sees fit. Though the Presidential executive order predates the Homeland Security Act of 2002, the council operates with the membership provided within the executive order.)

36. Ronald Reagan. Executive Order 12656: "Assignment of Emergency Preparedness Responsibilities," Washington DC: The White House, November 18, 1988; available from: *http://www.archives.gov/federal_register/executiveorders/1988.html*, Internet, accessed September 22, 2002.

37. Roger Corneretto, J7, Conventional War Plans Division, "War Plans Interagency Coordination," September 2002. The briefing highlights requirements of Annex V as a CJCS initiative required for all CJCS approved plans, and the NSC role was codified in November 1999 memorandum from then President Clinton to then Secretary of Defense Cohen. Annex V requirements serve three purposes:

> (1) part of a process by which we strengthen our ability to quickly and effectively respond to crises by ensuring integration of other instruments of national power into the Department of Defense deliberate planning process; (2) is the vehicle for CINCs to request interagency activities and lay the groundwork for the potential of coordinating with IOs, NGOs, and PVOs for participation. Obtaining coordination and integration to support the military objectives of the campaign; (3) articulates CINC's desires for entry and exit conditions for USG agencies during an operation." The briefing further states: An APNSA memo (24 April 2001) established four additional functional PCCs, including the Contingency Planning PCC (CP PCC). This PCC will manage the interagency process for reviewing Annex V's, produce political military plans, and plan for contingencies outside the deliberate planning cycle.

38. Colin Gray, *Modern Strategy*, Oxford, 1999, p. 358.

39. George W. Bush, "The National Strategy for Homeland Security," p. 5.