The US Army War College Quarterly: Parameters

Volume 31
Number 3 *Parameters Autumn 2001*

Article 8

8-17-2001

An Organizational Framework for Homeland Defense

Terrence Kelly

Recommended Citation

Terrence Kelly, "An Organizational Framework for Homeland Defense," *Parameters* 31, no. 3 (2001), doi:10.55540/0031-1723.2051.

An Organizational Framework for Homeland Defense

TERRENCE KELLY

From *Parameters*, Autumn 2001, pp. 105-16.

One of the most difficult problems facing government today is the question of how to organize to address new threats to national security. Noteworthy among these are threats from terrorism, proliferation of weapons of mass destruction, and attacks on our critical infrastructures. Others include the international drug trade, organized crime, and assorted transnational threats. These are nonconventional threats, and no single department or agency of the federal government can address them alone. They require coordinated policies, planning, and execution by agencies that fall on both the national security and domestic sides of the government, and they often involve cooperation with state and local governments, nongovernmental organizations (NGOs), and the private sector as well. Responses to them are crosscutting, involve non-federal organizations, and draw on assets that are already committed to other important missions. For the federal government, this creates problems of issue ownership ("turf"), and resource allocation--in both the annual President's Budget Submission, and in the congressional authorizations and appropriations processes. A lot of people have given a lot of thought to these issues, and it has become apparent that there will be no simple organizational solution.

Another important aspect of this problem of organizing for homeland defense is the difficult questions it raises about the role of government in society. When individual actors have the ability to launch cyber-attacks that shut down major corporations (as in February 2000) and madmen with modest assets can culture and spread pathogens that have the potential to kill thousands or even millions of citizens,[1] government must carefully consider how it should organize to address such potentially disastrous threats. In this process, important tradeoffs must be considered between catastrophic damage to the nation and an expanded (and possibly more intrusive) role for government. The prospect of an expanded government intruding on its citizens' rights is of such major importance that it must be addressed in full partnership with the Congress and, to the greatest extent possible, in open forums.

A Recommendation

A solution to this organizational issue can be based loosely on the military combatant command model.[2] In this model, the military's regional Commanders in Chief (CINCs) conduct operations (warfighting, peacekeeping, humanitarian operations) and report to the Secretary of Defense and the President. The forces they use to conduct these operations are raised, trained, and supplied by the military services. Almost all resources come through the military services as well.[3] And while the CINCs do not "own" the forces they use to conduct operations (these forces are assigned to them by the Secretary of Defense for specific missions), the CINCs have a loud voice in setting the requirements that shape them. In fact, the entire military model for the structuring and equipping of forces is driven by the requirements set by doctrine and warfighting demands. This model could provide a framework for solving some of the most pressing problems of organization and resource allocation for homeland defense. The framework could include:

- The creation of a Homeland Defense Agency (HDA) with a headquarters staff similar to that of a regional CINC.
- The identification of government agencies that could be permanently moved under the HDA without adversely affecting their home agency.
- The identification of government agencies that could not be permanently moved under the HDA without adversely affecting their home agency, and the establishment of habitual, plan-driven relationships with them to address specific homeland defense missions.

- The placement of the resource allocation decision authority for homeland defense issues that span more than one department or agency with the Vice President.
- The elevation of the position of National Coordinator for Security, Critical Infrastructure, and Counterterrorism to Assistant to the President, and the dual placement of this position under both the Vice President and National Security Advisor.
- The stipulation of specific engagement considerations.

The exact structure and missions of the Homeland Defense Agency would depend on the outcome of the debates on the larger issues concerning the role of government in society. The goal here is simply to recommend a framework, highlight important considerations, and stimulate discussion.

Background

It is useful to note that "homeland defense" has multiple meanings. In the context of this article, it indicates defense against new and yet-unknown threats that are not readily addressed by the existing military structure. Missions such as national missile defense, defeating traditional military forces that might invade the nation, and defense against strategic bombers would remain with the military. It will also become apparent that some overlap with military missions is unavoidable on issues such as cyber-defense, but these are manageable.

The current federal government policy center for issues of homeland defense is the National Security Council's National Coordinator for Security, Critical Infrastructure, and Counterterrorism (hereinafter the "National Coordinator"). Under the new NSC structure, these issues fall under the National Preparedness and Counter Terrorism Policy Coordination Committee. To connect policy to resources, the Office of Management and Budget established a "National Security Crosscut" that uses NSC subgroups to look at cross-governmental programs. It attempts to establish the requirements in each field, coordinate programs across the government to eliminate duplication and facilitate cooperation, and recommend a portfolio of programs to supplement those already ongoing in government that will fill the identified gaps and shortfalls. This combination of policy and coordination at the NSC, and budgeting (and to a lesser extent management) at OMB, represents an innovative attempt to avoid government by "czardoms," while integrating efforts across government.[4]

This model has had limited success because it suffers from three major shortcomings. First, it relies on the department and agency representatives serving on the National Preparedness and Counter Terrorism Policy Coordination Committee subgroups to check their departmental affiliation at the door. For most this is philosophically possible, but practically impossible. These groups are good at recognizing what is in the nation's best interest, but the process breaks down when actual funding priorities are brought into question. (One never hears an agency representative say, "I think you should have my funding--your program is more important than mine.") The members of these groups are answerable to the senior leaders of their departments or agencies, so they are understandably hesitant to recommend programs or policies that will not benefit or may even hurt their home agency. Agency representatives simply cannot do that without either consulting with their leaders (which is time-consuming and strips the interagency character from the resulting recommendations) or risking their careers.

The second major shortcoming of this process is that it has no teeth. These groups do in fact succeed in agreeing on recommendations for programs, but their recommendations are frequently not implemented. This is because the President's Budget Submission is constructed in stovepipes--department by department and agency by agency. To date, the policy process run by the NSC has not regularly engaged the department and agency leaders at the highest level to set resource allocation priorities, and OMB has not participated at a senior enough level to force these program recommendations through budget channels. The result is a lukewarm set of recommendations that has no support where it counts, at the highest policy and resource levels of the departments and agencies.

Despite these shortcomings, the process has had some success in getting specific, high-profile initiatives into the President's Budget Submission, usually through direct intervention by the National Coordinator. A third major shortcoming comes into play here to kill many of these initiatives, however. This is related to the stovepipes mentioned above, but is physically located at the other end of Pennsylvania Avenue. Just as in the executive branch, the House and Senate appropriations committees view the world though their individual stovepipes. These committees understandably focus on the areas for which they are responsible. Programs that require a broader perspective--those that do not fall neatly in any one of these stovepipes--tend to go wanting. The result is that multi-agency programs that are important to the nation and make it into the President's budget are frequently not funded or are only partially funded by the Congress.

Comparison of Options

This process clearly presents a difficult organizational problem. The key people in both the executive and legislative branches are, in general, deeply committed to doing the right thing, but they are hobbled by the difficulties of the process. A different organizational solution is needed. Outlined below are potential organizational solutions that either require no significant changes in the structure of the government, a major organizational change, or a somewhat less drastic organizational change that would largely mirror the military model mentioned above.

Solutions that would require only small changes to the organization of the government can be viewed as falling on a spectrum ranging from the traditional government by departments and agencies to the creation of one or more "czars" who have significant authority over policies and budgets. Options on this spectrum include some form of increased oversight and participation by senior officials on the White House Staff, or the creation of a Czar for Homeland Defense.

Increased participation by senior members of the White House staff--primarily the NSC (in the person of the National Coordinator) and OMB--would go a long way toward addressing the first two major shortcomings listed above. This does not come without a cost, however. Neither of these offices has the staff or resources to do this task well. Furthermore, structural changes would be required in each. This effort would require the elevation of the National Coordinator to at least the rank of Deputy Assistant to the President (roughly equivalent to a Deputy Department Secretary). OMB would need to give this mission to a new or existing Deputy Director (along with the associated resources) to provide the "teeth" for the effort. Both offices would need to be staffed appropriately. In addition to the political appearance problem of expanding the White House staff, this also would bring up the much more important issue of limits on the authority of White House staff officials. Put bluntly, giving a White House staffer not subject to congressional oversight operational or near-operational responsibilities is a non-starter. Furthermore, these solutions do not address the third shortcoming mentioned above. Congressional oversight and funding would retain their current form and continue to provide significant drawbacks.

The creation of a Homeland Defense Office and Director in the White House staff (the czar model) shares this last problem as well. Furthermore, government by czardom is not a popular notion, and for good reasons. Czars have no line responsibility, but have a vote on agencies' policies and budgets. Czars, while often confirmed by the Senate, typically do not fall squarely under the oversight of any single committee. The current congressional problems would continue to exist. Furthermore, government by czardom is not a well-thought-out management concept, but rather an attempt to make a cumbersome system more efficient. To date it has arguably had limited success. Other permutations of this type could be explored, but all would share these same drawbacks. Rather than tinkering around the edges of the organizational issue, it would be better to fix it.

A frequently mentioned but more drastic solution would be the creation of a Department of Homeland Defense.[5] This would involve moving assets that are critical to homeland defense out of their current organizations (e.g., the Federal Emergency Management Agency, the National Guard, Coast Guard, elements of the FBI), and placing them in this new department. Creating a Department of Homeland Defense would help solve all three shortcomings described above. It would establish a dedicated center of gravity for these issues with the ability to craft crosscutting policies and programs that address national rather than departmental issues. It would have a dedicated place in the President's Budget Submission like all other departments and agencies. And, because this would be a major part of the governmental structure, it would necessarily fall under the existing or some new committee structure on Capitol Hill. The responsible committees would then have to address these crosscutting policy and resource issues, thus establishing a "home" for homeland defense in the Congress.

But this option also would create as many problems as it would solve. Moving the aforementioned parts of existing government structures that address these threats into a new department would entail splitting up and damaging such critical bodies as the FBI (for example, moving its counterterrorism assets), the Department of Transportation (moving the Coast Guard), the Department of Defense (moving the National Guard), the Secret Service (moving some of its financial crimes assets), and the list goes on. This would not only cause significant internal upheaval in these departments and agencies, but it also would hurt their ability to perform their current jobs, since these pieces are not distinct and separate from the missions of their parent organizations. This could be mitigated by the duplication of these elements, but that would be prohibitively expensive and create new turf wars. In short, the creation of a Department of Homeland Defense would be a drastic step that would likely hurt the government's ability to perform other critical missions as much as it might help with homeland defense.

Fortunately, there is a reasonable solution short of creating a Department of Homeland Defense: the creation of Homeland Defense Agency (HDA) with a Senate-confirmed Director of cabinet rank. This agency would be modeled after the headquarters of the military's regional CINCs. It would consist of a staff that plans for operations in these specific areas, advises on policy issues, and controls operations when needed (analogous to the staffs of the CINCs). As recommended by the US Commission for National Security/21st Century, the Homeland Defense Agency should be built upon the Federal Emergency Management Agency (FEMA). It should absorb the FBI's National Infrastructure Protection Center, the Commerce Department's Critical Infrastructure Assurance Office, and the Justice Department's National Defense Preparedness Office. This would give it a core of operational and policy-support capabilities not firmly embedded in existing agencies, and improve coordination between these offices. And while no exhaustive list of assets that should be moved into the HDA can be finalized without significant cross-governmental analysis, it is clear that it should absorb no asset that is integral to existing and continuing departments or agencies and their missions.

Rather than tearing the guts out of several departments and agencies, assets needed for homeland defense would be assigned to the HDA for the conduct of training and operations in accordance with fixed plans, just as the military services assign forces to the CINCs to perform their missions.[6] Note that these would be formally identified assets and people, dedicated by the departments and agencies for specific missions. For example, a plan to counter bio-terrorism might call upon identified and dedicated personnel and organizations from the FBI (counterterrorism specialists), the Centers for Disease Control (pathologists and epidemiologists), the Customs Service, and so forth. The National Security Council would still oversee policy in these areas, but the HDA staff would play a major role in creating and recommending policy and strategy. This, too, closely mirrors the current military model, where policy is largely the domain of the senior civilian leaders in the Department of Defense and the NSC, but the military staffs and commanders play an active role in identifying requirements, advising on capabilities and limitations, and recommending options. Furthermore, homeland defense policy should be addressed in the President's annual National Security Strategy. And just as the military builds the National Military Strategy from the National Security Strategy, so too would a Homeland Defense Strategy be built to articulate the matching of ends, ways, and means in this domain. This system would result in the development of a cohesive policy and a responsive operational capability for homeland defense.

Policy, Strategy, and Criteria for Operations

As currently structured, the responsibility for developing homeland defense policy and strategy falls to the National Coordinator. This has significant benefits. This strategy necessarily involves multiple agencies across government, and the NSC is well-suited to coordinate it. This process also provides access to the President. There are other considerations, however, that must be addressed. The following discussion on operations and resources extends the analogy of the Homeland Defense Agency to military combatant commands, and it yields insights that need to be considered in determining who should be responsible for formulating homeland defense strategy.

As the CINCs are charged with developing the plans to meet the requirements of the National Security Strategy and National Military Strategy, so too should the Director of the Homeland Defense Agency be charged with developing plans and proposing a Homeland Defense Strategy. These homeland defense plans would draw on the assets and resources identified by various departments and agencies as discussed above. The Homeland Defense Agency would also need to conduct periodic training with the dedicated people and organizations from other agencies to ensure its ability to execute the homeland defense plans. These training exercises would engage the dedicated assets and help identify resource requirements. This would also help build the "command relationships" necessary for efficient execution in times of emergency.

Using this model, the Director of the Homeland Defense Agency would identify requirements for programs and capabilities to both OMB and the departments and agencies directly supporting the homeland defense plan for inclusion in the President's Budget Submission. Unlike the current system, the Director of the HDA would be there to champion these requests. Yet ultimately there would need to be a single office, short of the presidency, where competing resource demands between the HDA and the supporting departments and agencies could be adjudicated. Since this issue goes to the heart of defending the nation from potentially serious attack, and since significant operational and resource issues are involved, this responsibility ought to be vested in an official on the National Security Council who is senior to the department and agency heads that must cooperate. Short of creating a super-secretary who would sit over several departments and agencies, this leaves but one choice, the Vice President. And given that the Vice President would be the final arbiter of operational and resource issues for the HDA and associated departments and agencies, he or she should also play a major role in approving policy and strategy. To facilitate policy and strategy formulation, the National Coordinator should be dual-hatted under the NSC and the Vice President and elevated to the rank of Assistant to the President. This would give the position the access needed for success. It would also strongly link HDA policy to both the national security policy center, the NSC, and its proposed resource decisionmaking authority (and statutory NSC member), the Vice President.

As discussed for the Department of Homeland Defense, the Homeland Defense Agency would require congressional oversight and funding, and so would fall under some new or existing committees. These committees would necessarily assume policy responsibility for this cross-governmental issue for the legislative branch. Appropriations might still be spread across the subcommittees that fund the HDA and the associated departments and agencies, but with the oversight committee as designated interlocutor, more attention and focus would exist on the Hill for this important issue.

Developing criteria for the use of the HDA is also a critical issue. It is important to mention that barring unforeseeable changes in law, the Director could not have command authority over US military forces, and probably would not have directive authority over some other government agencies such as the FBI. He or she could, however, assign them missions and, in conjunction with the Secretary of Defense and the Attorney General (and perhaps other cabinet members), supervise their performance. Firm recommendations on the details of such arrangements must await the answers to the questions about the role of government in society alluded to in the introduction, but a few observations and considerations for employment of the Homeland Defense Agency are in order.[7]

The first is the connection between our national interests and HDA operations. Key here are the issues of civil and privacy rights, as well as relations with our allies and other major powers. These must be balanced with the level and immediacy of the threat of attack. To avoid major pitfalls, political goals and boundaries must be clearly understood by the HDA Director and key leaders. This would include consideration of the international effects of operations (e.g., regarding the pursuit of terrorists or cyber-villains across international boundaries), and the wisdom and necessity of conducting operations in conjunction with allies. The need to observe treaties and other bilateral or multilateral agreements also falls in this category. In the cyber case in particular, the deliberations would include a cost-benefit analysis of the economic, national security, and political ramifications of deterring an attack or punishing an attacker.

A review of existing policy and careful consideration of new proposals to align options for HDA operations with policy and strategy are also in order. Planning options must be weighed against operational capabilities, and the deterrent and antagonizing effects of specific operations considered. Allied cooperation would once again be important due to the international nature of these problems.

Another critical consideration is the balance between resources and operations. Sufficient resources will not exist to analyze and handle all situations, so clear guidelines and priorities must be in place to guide action. Finally, public and congressional opinion must be considered. This is not just to avoid embarrassing political altercations and news reports, but to forge a national consensus for long-term efforts that will increase the safety of the nation.

Government, Society, and New Security Institutions

The Homeland Defense Agency option has shortcomings as well, not the least of which is the cultural adjustment needed across government to make such an effort work. The military went through this change after the Goldwater-

Nichols Defense Reorganization Act became law in 1986, and the Defense Department emerged stronger. Similar benefit may accrue to the departments and agencies that work with the HDA. Yet there are valid concerns about the role of government in addressing these issues. Note that these shortcomings are not unique to the HDA--they would be shared by any comprehensive solution. Among these are such fundamental questions as the role of government in society and our people's expectations of privacy. It would be premature to propose solutions to any of these issues without full and open debate. Yet some fundamental observations and questions can be addressed here.

Underlying this discussion is a trend indicating that the know-how, technology, and ultimately the ability to create significant or even catastrophic damage is increasingly in the hands of greater numbers of people, while far fewer people are needed to cause this damage.[8] There is little doubt that a knowledgeable hacker with a cheap personal computer can inflict millions if not billions of dollars of damage to businesses on the internet, and a lunatic with modest resources may be able to create and spread dangerous pathogens. Note as well that Western societies are founded on the fundamental philosophical principle that all power comes from the people, who cede portions of it (and therefore some of their freedoms) to government so that it can ensure their safety, welfare, and potential for prosperity. These two observations suggest that new, nontraditional threats pose risks to all societies of a magnitude heretofore unknown, and that solutions may require the ceding of additional liberties. There is a point beyond which most individuals would not willingly cede more power and freedoms to the government. For each individual, however, this is a fuzzy line, and for society as a whole it presents a very difficult question. It may be closely linked to related questions, such as the magnitude and imminence of a threat and the need to identify and defeat it. The relative roles of private entities and government must also be considered. Answers to these issues are not clear, but they will both enable and bound the actions of the HDA. In considering them, it is necessary to examine some fundamental values and trade-offs, and to ask important questions.

One such question involves the role of the intelligence community in tracking the perpetrators of homeland threats. Without good intelligence, government cannot know the magnitude and imminence of the threat and will be poorly postured to identify and defeat it. But strict prohibitions exist on the latitude of the military and CIA to collect intelligence on US citizens, and indeed on anyone within US borders. This is the domain of the FBI and Justice Department, under the oversight of the courts. Yet our increasingly global existence, where travel is relatively easy and communications are instantaneous and without boundaries, puts a real strain on the ability of the intelligence community to quickly develop and disseminate the intelligence it might need to stop a terrorist, weapons of mass destruction, or a cyber-attack. To what extent are US restrictions against domestic intelligence collection still sensible? What level of threat would warrant overturning them? Do the mechanisms currently being developed to streamline intelligence-sharing make these restrictions moot or alter these considerations? Do we need a thorough review of the legal and logical questions associated with intelligence matters in the 21st century?

A second consideration involves the role of the military. The Posse Comitatus Act was passed after the Civil War in a congressional compromise to get Union soldiers out of the business of performing government functions in the South during Reconstruction.[9] Yet in the areas of terrorism, weapons of mass destruction, and cyber-attacks, the military possesses significant capabilities and brings to bear important resources for monitoring, tracking, locating, and potentially retaliating against attackers. This is particularly noteworthy in the cyber domain, where military skills are several years ahead of the rest of the government (though not the private sector) and where military cyber-intervention would be much less intrusive than in the more physically based domains of terrorists and weapons of mass destruction. Is Posse Comitatus still appropriate? What are the societal and political ramifications of changing or rescinding it? In the context of each of these new threats, what is the "battlefield"? What should be the role of the National Guard in homeland defense? What would be the effect on other core military missions?

Another issue involves the nature of cyberspace and privacy rights. This is a two-edged sword. In order to protect private information, institutions must be able to identify intruders. Recent pieces of legislation, such as the Health Insurance Portability and Accountability Act and the Gramm, Leach, Bliley Act, address this issue by setting the groundwork for holding corporations responsible for safeguarding the health and financial information, respectively, of their clients. Yet to do this they must construct significant cyber protections, and this may require collecting information about people using their systems. This raises significant privacy concerns. Furthermore, this issue is even more sensitive when it is government collecting this information. People are rightly concerned about the ability of the government to amass and misuse encyclopedic information on its citizens. The potential for abuse is significant and must be guarded against. What level of monitoring should be allowed by private firms and the government? Can information be collected and abuses prevented? Should institutions be held responsible for safeguarding private information if they are denied the tools with which to do it? What are the trade-offs?

A fourth concern again involves the nature of cyberspace, and the fact that to do almost anything on the internet requires using intermediate nodes spread around the globe. This raises important legal, policy, and ethical questions about a government's use of the internet to track domestic and international malefactors. For example, during the recent Israeli-Palestinian dispute, it was reported that an American corporation providing internet service to the Israeli government was contractually bound to help defend the networks from attacks by Palestinian sympathizers--and that US supporters of both sides had used facilities at their American business worksites to launch attacks on their opponent's systems. The international governmental and corporate liability questions implied by these reports are uncharted territory in which proactive, well-thought-out policy and legislation is needed before a crisis occurs.

Related to the global nature of the internet and the speed of operations in cyberspace are questions of jurisdiction and due process. Hunting down hackers or other malicious actors on the internet currently requires warrants in all jurisdictions through which the attack passed, and cooperation with foreign governments when the path is international (which is almost always the case). Should there be "national warrants," as the Justice Department has called for, to speed this process within the United States? Should we sign treaties that permit us access to other nations' infrastructures for this purpose, with the understanding that such treaties would give other governments (or multinational organizations such as the UN) access to our infrastructures as well? What is to be gained and what rights would be lost should such policies be adopted?

Information sharing is another critical issue for the pursuit of international malefactors. Private-sector organizations may have information that would benefit the government's efforts to pursue, arrest, and prosecute terrorists or cyber-villains, but may be hesitant to share it with government for fear that proprietary information could be exposed through Freedom of Information Act requests.[10] Information sharing is also encouraged between private corporations to increase overall security, but this raises concerns for anti-competitive behavior. Finally, information sharing brings the possibility of lawsuits for failure of due diligence. Are legislative or regulatory changes needed to address such concerns?

These are but a few of the tough questions that must be asked and answered in order to craft an effective organization and associated policy for dealing with these new threats.

Conclusion

A few points are clear. First, the federal government, at both ends of Pennsylvania Avenue, is poorly organized to facilitate a national defense against these new threats to national security. Attempts to adjust the current architecture to meet these new challenges have been remarkable for their limited success in the face of severe obstacles, but have still fallen short. A Homeland Defense Agency, modeled roughly after the military's combatant command structure, is needed to orchestrate efforts across government, while at the same time minimally detracting from the other requirements of the affected departments and agencies. A reorganization of the White House Staff is needed to ensure proper policy and strategy oversight. This can be accomplished by placing the current National Coordinator under both the NSC and the Vice President, and elevating the position to the rank of Assistant to the President. Finally, the role of the Homeland Defense Agency will depend upon the resolution of significant policy, legal, and value discussions that go straight to the heart of the role of government in our society. In the face of these new and potentially catastrophic threats, it is important to advance these efforts and discussions.

NOTES

1. For example, the US Commission on National Security/21st Century states in *Road Map for National Security: Imperative for Change*, p. 4: "A few people with as little as $50,000 investment may manage to produce and spread a genetically-altered pathogen." Internet, www.nssg.gov, accessed 13 June 2001.

2. Special thanks to Dr. Vigdor Teplitz, who first suggested looking at the "CINC model" for this problem.

3. A notable exception is Special Forces Command. The focus in this article is on the more usual model used by the geographic CINCs.

4. The Director of the Office of Drug Control Policy is the best current example of an issue-area czar.

5. The third report of the US Commission on National Security/21st Century, *Road Map for National Security: Imperative for Change*, recommends this approach. The Commission's ideas for a National Homeland Security Agency (NHSA) are compelling, but see the drawbacks identified below.

6. The forces used by the CINCs to conduct operations actually belong to the Army, Navy, Air Force, and Marine Corps. They are aligned against specific operation plans devised by the CINCs for the execution of their responsibilities, and allocated to the combatant commands by the Secretary of Defense.

7. These are based on the framework presented by John Collins in "Military Intervention: A Checklist of Key Considerations," *Parameters,* 25 (Winter 1995-1996), 53-58.

8. Keith Gardner, "Toxic Knowledge," unpublished paper from the Deputy Assistant Secretary General for Scientific & Environmental Affairs, NATO Headquarters.

9. 18 US Code, Section 1385.

10. Freedom of Information Act (FOIA) requests allow citizens to get information held by the government and are a key component of an open, "transparent" system of government.

Lieutenant Colonel Terrence Kelly, Ph.D., is the Senior National Security Officer in the White House Office of Science and Technology Policy. He served in the 82d Airborne Division, the 8th Infantry Division, on the Army Staff (ODCSOPS), on the faculty of the US Military Academy, and more recently as a White House Fellow, with Army Legislative Affairs, and as Chief of Staff of the interagency Critical Infrastructure Assurance Office. He has a Ph.D. in mathematics and an M.S. in computer and systems engineering from Rensselaer Polytechnic Institute, and he is a 1982 graduate of the US Military Academy.

Reviewed 15 August 2001. Please send comments or corrections to carl_Parameters@conus.army.mil