Report to Congress
on
The Role of the Department of Defense in Supporting Homeland Security

September 2003

Pursuant to Section 1404 of the
National Defense Authorization Act for Fiscal Year 2003

Table of Contents

Report to Congress on

The Role of the Department of Defense in Supporting Homeland Security

required by

FY 2003 National Defense Authorization Act (NDAA), Section 1404

DEFINITION OF THE DOD HOMELAND SECURITY MISSION

Homeland security is a concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, minimize damage, and assist in the recovery from attacks. The Department of Defense (DoD) role in homeland security can be summarized as follows: (1) **homeland defense**, the military protection of United States territory, domestic population, and critical defense infrastructure and assets from external threats and aggression; and (2) **civil support**, support to U.S. civil authorities for domestic emergencies and for designated law enforcement and other activities. Civil support missions are undertaken by the Department where its involvement is appropriate and where a clear end state for the Department's role is defined. The Department will seek reimbursement for civil support missions when authorized by law.

Defense of the U.S. has always been and remains DoD's primary mission. DoD maintains forces sufficient to conduct operations abroad while protecting the U.S. domestic population, its territory, and its critical defense-related infrastructure against attacks, as appropriate under U.S. law.

Additionally, DoD has provided various kinds of support to civilian authorities throughout its history. DoD will continue to provide such support as directed by law and in accordance with the National Response Plan, when approved. Recent events have prompted shifts in demand that require changes in operational emphasis. For example, the President created the U.S. Northern Command (NORTHCOM) in order to improve command and control of DoD forces in homeland defense and civil support missions.

DoD takes a broad view to ensure preparedness to meet its global requirements for national defense. Its responsibility to protect its personnel and resources remains unchanged. The Department will continue to ensure the full mission readiness of each combatant command through policy development and oversight, program planning, allocation of resources, and mission execution oversight.

Coordination with authorities at all appropriate levels will be the key to achieving both our homeland defense and our civil support objectives. In the intergovernmental community at the federal, state, and local levels, DoD continues to develop close and collaborative relationships to ensure that the Department's efforts, when appropriate, support and reinforce civilian contingency plans and resources. Similarly, within the Department, coordination is essential on matters such as intelligence, investigations, research and development, health, reserve affairs, education, training, mission planning, mission rehearsal, and operational employment.

CHANGES TO ROLES, MISSIONS, RESPONSIBILITIES, ORGANIZATION, AND CAPABILITIES

Office of the Secretary of Defense

Two major changes have taken place within the Office of the Secretary of Defense. The Assistant Secretary of Defense for Homeland Defense (ASD(HD)) has been established to provide overall supervision of the homeland defense and civil support activities of the Department. Additionally, the new Under Secretary for Intelligence (USD(I)) is the principal intelligence official within the Department.

Assistant Secretary of Defense for Homeland Defense. The mission of this new office, which is located within the office of the Under Secretary of Defense for Policy, is to provide overall supervision of the Department's homeland defense activities, ensure internal coordination of DoD policy direction, assist the Secretary in providing policy guidance through the CJCS to the appropriate combatant commanders for the homeland defense and civil support missions, and provide for coordination with the Department of Homeland Security (DHS) and other government agencies. It is also the focal point for DoD's interaction with the Homeland Security Council, relevant activities of the National Security Council, DHS, and the interagency community for homeland security issues. Section 902 of the FY03 NDAA authorized the Secretary of Defense to establish an ASD(HD).

The office of the ASD(HD) is a policy-based organization focused on building and improving DoD's efforts in supporting the nation's homeland security requirements. The organization unifies DoD's homeland defense, military support to civil authorities, and emergency preparedness activities by providing focused management, oversight, and supervision of policies, programs, and resources.

Specifically, the new office is responsible for:

- Overall supervision of DoD homeland defense activities.
- Developing strategic planning guidance for DoD's role in homeland defense and civil support.
- Developing and updating domestic force employment policy, guidance, and oversight related to homeland defense and civil support missions.
- Overseeing DoD preparedness activities to support civil authorities in domestic emergencies in accordance with the existing emergency response plans or the National Response Plan proposed by the President.
- Providing DoD support, as appropriate, to assist civilian agencies in developing capacities and capabilities required to conduct domestic homeland security missions.

- Serving as the DoD Domestic Crisis manager to focus the coordination and integration of DoD domestic crisis activities with other departments and agencies and the combatant commanders, except for those activities requiring the use of special operations forces.

The ASD(HD) will maintain close working relationships with the Principal Staff Assistants throughout DoD who hold responsibilities for capabilities relevant to homeland defense, civil support, and emergency preparedness. On matters such as research and development, critical infrastructure protection, health affairs, reserve affairs, and intelligence, the ASD(HD) will help integrate departmental efforts in order to maximize the full range of homeland security capabilities.

Domestic antiterrorism and force protection (AT/FP) remain responsibilities of the service components and installation commands. The role of NORTHCOM in AT/FP is under development. Counterterrorism will continue to be the responsibility of the ASD for Special Operations/Low-Intensity Conflict (SO/LIC). In extraordinary cases where special operations counterterrorism forces are called upon by the President to undertake a military operation within the United States, the ASD(SO/LIC) will serve as a principal advisor to the Secretary of Defense, in coordination with the ASD(HD). For domestic consequence management, which may include responses to acts of terrorism and manmade or natural disasters, the ASD(HD) will exercise oversight and supervision of contingency planning for military support to civil authorities.

Under Secretary of Defense for Intelligence. Section 901 of the FY03 Defense Authorization Act provided for the creation of the USD(I). This major reorganization of defense intelligence oversight will ensure greater cohesion in the management of the many intelligence capabilities currently within DoD, enabling it to provide more coordinated, better focused intelligence support for pressing national concerns like homeland security. The USD(I) will work with the intelligence community and will maintain a close relationship with the ASD(HD), providing an opportunity for feedback regarding intelligence tasking, processing, exploitation, and dissemination as it affects homeland defense/security users at various levels.

The USD(I) will ensure that defense intelligence is fully integrated with and responsive to the national intelligence mission and that the Department has an effective working relationship with the Office of the Director of Central Intelligence. The office of the USD(I) will be primarily responsible for ensuring that the Department, including the Military Services, combatant commands, and other DoD agencies, activities, and elements, receives the warning, intelligence, security, and the counterintelligence support needed to pursue the objectives of the nation's defense strategy. For homeland security-related matters, the new office will enhance DoD's intelligence-related activities, provide a primary point of contact for coordination of national and military intelligence activities with the staff of the Director of Central Intelligence, and strengthen the relationship between the Secretary of Defense and the Director of Central Intelligence.

Military Services

The role of the Military Services in supporting homeland security-related functions (i.e., homeland defense and support to civilian authorities) has not changed in recent years. The

Services' primary responsibility is to prepare forces to fight and win the nation's wars. To maintain its warfighting capability, the Services focus on organizing, training, and equipping units for employment by the combatant commands. This focus also gives the Services the capability to fulfill a variety of homeland security-related functions. These functions span a range of missions that could include the traditional warfighting requirements associated with defeating an external threat, to the non-combat tasks associated with supporting civil authorities in domestic consequence management for natural disasters and terrorist attacks.

In the homeland defense mission area, the Services provide NORTHCOM and PACOM with the capabilities to perform the traditional uniformed military service missions to defend its Area of Responsibility, to include the air, maritime, and land approaches into the nation as well as to protect designated critical infrastructure. The primary orientation for homeland defense is defending against external threats and aggression. But under extraordinary circumstances there are cases in which the President, exercising his constitutional authority, could authorize military action to counter threats within the U.S.

Because of their wide range of capabilities and geographic dispersion across the country, the Military Services are uniquely capable of providing NORTHCOM and PACOM with capabilities for supporting civil authorities across a spectrum of domestic contingencies, when directed by the President or the Secretary of Defense. The Services provide NORTHCOM with the capability to support civil authorities who do not possess the necessary capabilities or whose resources are overwhelmed or exhausted. Support to civil authorities generally can be described in three categories:

- Military Assistance to Civil Authorities (MACA). Local and state governments have primary authority to respond to the consequences of accidental or deliberate Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives (CBRNE) incidents. Under appropriate circumstances, the federal government provides assistance consistent with its constitutional and statutory responsibilities. Under current policy, military support will normally be provided only when federal, state, and local resources are unavailable and only if the support does not interfere with the Military Services' primary missions or ability to respond to operational contingencies. The MACA category includes but is not limited to natural disasters and/or emergencies, manmade disasters, National Special Security Events/other special events, and CBRNE consequence management.
- Military Support to Civil Law Enforcement (MSCLEA). The MSCLEA category includes but is not limited to border patrol augmentees, National Special Security Events, support for counterdrug operations, support for combating terrorism, and general support such as training support and loan of equipment to law enforcement agencies, and national critical infrastructure protection. Military forces may provide support to civilian law enforcement agencies, consistent with the U.S. Constitution, statutes, and applicable policy.
- Military Assistance for Civil Disturbances (MACDIS). Military forces may provide support to federal law enforcement officials, consistent with the U.S. Constitution, statutes, and applicable policy.

While the Services' roles and missions in support of homeland security have not changed, they have provided an increased number of forces to homeland defense to meet growing requirements, to include providing air defense and maintaining quick reaction forces to respond to security incidents.

In the wake of the September 11 attacks, the Services have supported border security missions and disaster response requirements by augmenting civil agencies. As the capabilities of civil authorities increased, or support requirements were met through other means, the Services were able to reduce their commitments.

Army. The Army continues to perform a critical role in defending America. While the Army's roles and missions in support of homeland security have not changed, the Army has been providing an increased number of units and soldiers in support of homeland security-related missions to meet increased requirements.

In the areas of homeland defense and civil support, the Army's requirements and responsibilities have increased in response to threats to the nation's security. The Army maintains reaction forces on a graduated response posture ready to support HD missions. The Army also identified multiple units ready to provide consequence management augmentation for Joint Task Force-Civil Support (JTF-CS), if required and directed by the Secretary of Defense. The Army continues to identify units ready to support the DoD Civil Disturbance Plan should that be required and directed by the Secretary of Defense.

The Army currently provides ground-based air defense artillery units in support of the air defense of the National Capital Region. Army air defense forces from both active and reserve components continue to provide invaluable service in homeland security. Currently, both components provide protection to the National Capital Region by operating both ground-based air defense weapons and surveillance systems. The Army, in collaboration with the Air Force, is developing enhanced capabilities to protect multiple sites within the homeland from air attack. In addition to those soldiers physically defending our nation's capital, soldiers are serving as liaisons to appropriate NORAD Air Defense sectors, regions, and NORAD headquarters to ensure the seamless integration of ground-based and aerial defenses.

An Army core competency is to support civil authorities. Much of what the Army has done in support of homeland security-related missions over the past year has involved supporting civil authorities whose own capabilities have been exhausted or overwhelmed. The Army supported border security missions and disaster response requirements by augmenting civil agencies when their requirements exceeded their capabilities. As the capabilities of civil authorities increased, or support requirements we ne through other means, the Army was able to reduce its commitments. Because of its wide range of capabilities and geographic dispersion across the country, the Army is uniquely capable of supporting civil authorities across a wide spectrum of domestic contingencies.

In terms of force structure and organization, the Army made selected changes as a direct result of homeland security-related requirements. Recent changes to the force structure reflect these

requirements and include a new office on the Army Staff, the Army Service Component for NORTHCOM, the Army National Guard Restructuring Initiative, and the CBRNE Command.

The Army Staff is reorganizing to meet the emerging requirements associated with homeland defense and civil support. Concurrent with the establishment of the ASD(HD), the Army's interim DoD Executive Agent responsibilities for homeland security transferred from the Secretary of the Army to the ASD(HD). In response to this change, the Army established the Domestic Strategy and Support Directorate (DAMO-DS) within the Army G3 Staff to address homeland defense and civil support planning and coordination across the Army Staff and with the Joint Staff, other Services, combatant commands, and various federal agencies.

With the establishment of NORTHCOM, the Commander, U.S. Forces Command (FORSCOM) serves in the role of the Army Service Component Commander for NORTHCOM. Headquarters, FORSCOM retains its role as a force provider and remains assigned to U.S. Joint Forces Command (JFCOM).

The Army National Guard Restructuring Initiatives are designed to meet the requirements of the new and emerging defense strategy. The restructuring will create lighter, more flexible units with the introduction of two new types of organizations into the force structure—mobile light brigades and multi-functional divisions. The restructured Army National Guard units will remain fully capable of conducting combat operations to meet warfighting requirements for the regional combatant commanders while also addressing the unique needs associated with homeland security requirements. The restructuring initiative will begin in 2008 and should be completed by 2012.

Following the September 11, 2001 terrorist attacks, the Army recognized a need to focus command and control of its disparate CBRNE response organizations. Accordingly, the Army is designing CBRNE Command to manage existing CBRNE response assets with initial operational capability planned for June 30, 2004. CBRNE Command will integrate, coordinate, deploy, and provide trained and ready full-spectrum CBRNE and explosive ordnance disposal (EOD) response forces. CBRNE Command will be prepared to exercise command and control of full spectrum CBRNE and EOD operations in support of Joint and Army Force Commanders and provide Army support to civil authorities. CBRNE Command will maintain technical links with appropriate joint, federal, and state CBRNE/EOD assets, as well as research, development, and technical communities to assure Army CBRNE/EOD response readiness. As an interim measure until approval of the FY04 defense budget, the Soldier Biological Chemical Command (SBCCOM) is provisionally organizing a brigade-level organization (the Guardian Brigade) that will be placed under FORSCOM's operational control until CBRNE Command reaches initial operational capacity.

Navy. The Navy has been tasked to support NORTHCOM's mission to deter and defend against hostile action from maritime threats by providing defense in depth that is seamless, unpredictable to our enemies, and able to defeat threats at a maximum distance from U.S. territory. The Navy maintains alert ships and aircraft on both coasts and the Gulf of Mexico for this mission. The homeland defense Navy component is NAVNORTH, which reports to NORTHCOM. The forces for NAVNORTH will come from the Atlantic and Pacific Fleets, as determined by the

Secretary of Defense. The Navy also supports the United States Coast Guard (USCG) in its homeland security mission.

The Navy, the USCG, and federal agencies are working to establish a common Maritime Domain Awareness (MDA). MDA is the effective knowledge of all activities and elements in the maritime domain that threaten the safety, security, or environment of the U.S. or its citizens. MDA is accomplished by a national effort that integrates forward deployed naval forces with the other military services, civil authorities, and intelligence and law-enforcement agencies. This effort will ensure timely dissemination of actionable intelligence, and provide recommended courses of action to reduce vulnerabilities.

Naval forces conduct civil support missions for a Lead Federal Agency (LFA) by supporting law enforcement as well as providing complementary measures to protect public health, restore essential public services, and provide emergency relief to those affected by the consequences of disasters or catastrophes, either manmade or natural. For example, hospital ships, amphibious ships, and deployable Field Surgical Hospitals can provide large-scale medical facilities when local hospitals are damaged or overwhelmed.

Air Force. As with the other Services, the Air Force's role in national defense has not changed. Its core mission remains to prepare forces to conduct effective military operations in pursuit of the National Security Strategy. The Air Force champions six distinctive capabilities: Air and Space Superiority, Global Attack, Rapid Global Mobility, Precision Engagement, Information Superiority, and Agile Combat Support.

The Commander, Air Combat Command serves as the Air Force component commander to NORTHCOM. Additionally, the Air Force makes significant contributions of facilities and manpower to NORTHCOM. The Command is housed at Peterson Air Force Base and commanded by General Ralph Eberhart, USAF.

The Air Force has increased its 24/7 capabilities in a variety of ways to respond to federal taskings under Title 10 and non-federal taskings and Title 32 (federally funded, state controlled) authorities. Through extensive mobilization of Guard and Reserve resources, the Air Force has brought more than 30,000 airmen to full-time status, mostly in support of the increased national homeland defense posture. The Aircraft Alert Posture has more than doubled from 7 sites to 16 sites since September 11, 2001. Combat air patrols are employed for national security special events (NSSEs) and other designated public venues, as required. Also, the Air Force Auxiliary (Civil Air Patrol) has been reenergized to provide additional capacity to support NORTHCOM, other federal agencies, and state and local governments. This action utilizes approximately 62,000 non-paid volunteers and over 1,400 units located throughout all 50 states, the District of Columbia, and Puerto Rico.

North American Aerospace Defense Command (NORAD). NORAD forces are postured to ensure air warning and control for the continental United States, Canada, and Alaska. NORAD maintains an extensive radar system around North America and has alert fighters deployed throughout the United States and Canada that can respond quickly to threats. NORAD defends North America from domestic air threats through Operation NOBLE EAGLE. Across the United

States and Canada, armed fighters are on alert and flying irregular combat air patrols to identify and intercept suspect aircraft. Since September 11, 2001, NORAD has flown over 30,000 sorties to deter, prevent, and defend against potential terrorist attacks. The National Guard flies the vast majority of the sorties.

Marine Corps. The Commander, Marine Forces Atlantic is the Marine Corps component of NORTHCOM. Capabilities include the Chemical, Biological Incident Response Force (CBIRF) and the 4th Marine Expeditionary Brigade (4th MEB). The 4th MEB provides commanders with rapidly deployable, specially trained and sustainable forces that are capable of detecting terrorist activities, providing deterrence to terrorist acts, defending designated facilities against terrorism, and conducting initial incident response in the event of a chemical, biological, radiological, or nuclear terrorist attack worldwide. The Marine Corps also provides Quick/Rapid Reaction Forces in support of homeland defense.

National Guard. National Guard units play a prominent role in homeland security because of their ability to be employed in a federal or a non-federal status. The National Guard is often employed in a non-federal status, under state law, to meet the needs of state and local authorities. For example, the National Guard deployed to airports in the months following the September 11, 2001 terrorist attacks while the guardsmen remained under the direction and control of their respective governors.

Within the National Guard are the Weapons of Mass Destruction Civil Support Teams (WMD-CSTs). Congress directed the establishment of the WMD-CSTs in October 1998. A WMD-CST is a small National Guard unit that has been specifically trained, equipped, and organized to support local, state, and federal agencies responding to an attack involving chemical, biological, or radiological weapons. Due to the required level of training and expertise, and the requirement for rapid deployment, full-time members of the Army and Air National Guard staff the WMD-CSTs. Currently there are 32 certified WMD-CSTs and the Congress has authorized the establishment of 23 more.

The National Guard is postured to provide support and information sharing to NORTHCOM, PACOM, and SOUTHCOM, in accordance with existing law and as required. Fostering support and cooperation among U.S. homeland security DoD partners in the respective AORs is essential to countering terrorism and advancing U.S. national interests. NGB will use various methods to meet the challenge of providing near real-time situational awareness from the local to the national level as the official channel of communication with the several states, territories, and the District of Columbia.

Combatant commands

U.S. Northern Command. NORTHCOM was established on October 1, 2002 at Peterson Air Force Base, Colorado. NORTHCOM plans, organizes, and executes homeland defense and civil support missions. The command employs forces whenever necessary to execute missions as ordered by the President. The Commander, USNORTHCOM, is responsible for land, maritime, and aerospace defense of the territory and people of the continental United States, Alaska, Puerto Rico, and the U.S. Virgin Islands against external threats. When directed by the Secretary of

Defense, NORTHCOM provides military assistance to U.S. civil authorities. NORTHCOM is coordinating operational relationships to facilitate planning for employment of DoD units in support of the Command's assigned missions.

U.S. Southern Command: SOUTHCOM conducts military operations and security cooperation activities in support of the war on terrorism. SOUTHCOM combats terrorism primarily by supporting a determined Colombian government in their fight against narco-terrorist groups. The clear linkage between terrorism and illicit drug trafficking activities reinforces SOUTHCOM's critical role in deterring terrorist activities at their source, in support of homeland defense. SOUTHCOM's top command priority is to successfully prosecute the war on terrorism in its Area of Responsibility (AOR).

SOUTHCOM is postured to provide support to NORTHCOM as required. Fostering support and cooperation among partner nations in the SOUTHCOM AOR is essential to countering terrorism and advancing U.S. national interests. SOUTHCOM will use various methods to meet the challenge of eliminating transnational terrorism. For example, Operation ENDURING FRIENDSHIP, a maritime force of the Americas, when matured, could be instrumental in fostering regional maritime cooperation between hemispheric navies, coast guards, customs, and police forces. It could strengthen operational and planning capabilities of partner nations' national command and control systems, and promote regional information sharing.

Other Combatant Commands. JFCOM's role in support of homeland defense may increase in scope to include such matters as developing joint doctrine, training, etc. U.S. Pacific Command (PACOM) has homeland defense and MACA responsibilities for Hawaii and the U.S. territories in the Pacific.

Intelligence components

Collection and analysis of homeland security intelligence and information. The primary focus of intelligence collection and analysis within the Department is on the foreign threat and on the generation of intelligence for the protection of U.S. forces at home and abroad. Although terrorism that targets the homeland is fundamentally a law enforcement matter that is best addressed by domestic law enforcement entities with DoD in a supporting role during crises, the Department has a responsibility to protect its forces, capabilities, and infrastructure within the United States. Along with Service and DoD law enforcement/counterintelligence organizations and NORTHCOM, many federal, state, and local organizations outside the Department have leading roles in collecting and analyzing information and intelligence, and in conducting investigations and operations to prevent or preempt terrorist attacks.

The Defense Intelligence Agency's (DIA) Joint Intelligence Task Force–Combating Terrorism (JITF-CT) is DoD's lead national-level intelligence organization for indications and warning, the production of timely all-source intelligence, integration of national-level analytic efforts on all aspects of the terrorist threat, and development and maintenance of an accurate, up-to-date knowledge base on terrorism-related information. The Director, JITF-CT also serves as the DoD focal point and senior Defense Intelligence representative within the Intelligence Community (IC) for terrorist threat warning, proposing and coordinating within the IC promulgation of such

warnings to appropriate DoD organizations and combatant commands. The JITF-CT mission continues to evolve in consonance with other organizations involved in homeland defense/security, including NORTHCOM and the Department of Homeland Security, as an appropriate division of labor is worked out and as working relationships and data-sharing arrangements are established.

DIA's Directorate for Human Intelligence, meanwhile, collects foreign intelligence on international terrorist groups, not only in support of the homeland security mission but also in support of overseas U.S. military force protection and combat support missions.

In addition to the activities in the counterterrorism arena, DIA and the Intelligence Community provide assessments and warning analysis of cyber threats to the U.S. in general, and to DoD networks and systems in particular. This work characterizes the capabilities of various nation states and non-national organizations (such as terrorist and hacker groups) to conduct cyber attacks against critical infrastructures.

DIA supports homeland security in two other unique areas. The first is the tracking of weapons and materiel—including foreign sources of explosives—used by terrorists in their operations. The second is in the area of consequence management intelligence which the agency has worked for some time. This analysis focuses both on areas where U.S. forces are stationed or engaged, and on the homeland itself.

DoD law enforcement/counterintelligence elements are authorized, in accordance with their force protection and combating terrorism mission, to collect and analyze information on international terrorist threats in the United States as well as overseas. Key to the mission of DoD's Counterintelligence Field Activity (CIFA) is identification and tracking of terrorists and production of CI threat assessments and advisories and risk assessments in support of DoD force protection and critical infrastructure protection efforts, and tailored analytical and data-mining support to DoD CI field elements and agencies and the Service secretaries. These "knowledge products" provide a foundation for actions that can be taken to mitigate risks and enhance the security of U.S. persons, and critical operations, resources, and technologies. Central to CIFA operations is close collaboration and partnering with other organizations in the national intelligence and investigative community. CIFA is now furnishing a counterintelligence support team to assist the Federal Bureau of Investigation (FBI)-led Foreign Terrorist Tracking Task Force and is orchestrating the permanent assignment of DoD law enforcement and counterintelligence agents and analysts to the FBI's Joint Terrorism Task Forces throughout the United States. These personnel will collect and analyze terrorist threat and criminal information and participate in the investigation of international terrorist incidents having a DoD link.

The National Security Agency (NSA) and the National Imagery and Mapping Agency (NIMA) provide foreign intelligence support both to homeland defense/security missions and to U.S. activities overseas to prevent or preempt foreign terrorist planning and operations before they reach U.S. territory. The collection and analysis capabilities of these two organizations are also routinely called upon to support special national and international events, such as Presidential travel, Presidential inaugurations, Olympic games, and humanitarian missions over the United States, all of which have taken on homeland security dimensions. NIMA and NSA (as well as

DIA), for example, provided extensive support during the Salt Lake City Olympics, and in September 2001, NIMA conducted detailed toxic plume analysis over the World Trade Center sites in support of the Federal Emergency Management Agency (FEMA). In addition, all-source organizations involved in terrorism-related analysis, such as JITF-CT and NORTHCOM's Combined Intelligence and Fusion Center (CIFC), routinely draw from NSA and NIMA specialized collection and analysis efforts.

NIMA's North America and Homeland Security Division is collecting, developing, and disseminating the necessary Geospatial Intelligence (GEOINT) that is required to serve as the Common Operational Picture (COP) for DoD and all other U.S. government elements in their homeland security activities to include protecting the national critical infrastructure. The data assembled for the COP is being utilized for the production of a new line of GEOINT products including detailed data and analysis over 133 U.S. urban areas, critical infrastructure, and U.S. borders and coastlines required by NORTHCOM and others to support homeland security planning and exercises within these areas.

NORAD-NORTHCOM's CIFC has a clear-cut intelligence analysis responsibility, which includes the fusion of intelligence, law enforcement, and other domestic (e.g., medical) information into all-source, predictive, and actionable threat assessments to support NORTHCOM operations and protect NORTHCOM forces. In conducting this analysis, CIFC relies principally on reachback support from JITF-CT but also more broadly on traditional DoD intelligence sources, such as DIA, NIMA, NSA, and Service intelligence centers and other sources of DoD intelligence and information, such as the FBI and state and local law enforcement agencies. Other sources of homeland defense/security-related intelligence are the Combatant Command Joint Intelligence Centers (JICs)/Joint Analysis Center (JAC), which are responsible for warning and threat assessments related to their respective theaters of operation and lines of communication to the U.S. The Combatant Commands with geographic responsibilities provide indications and warning coordination and handoff to NORTHCOM any threats transiting their AORs toward the United States.

NORTHCOM is working closely with the DoD counterintelligence community, primarily with CIFA, to ensure it receives appropriate counterintelligence, counter-terrorism, and law enforcement reporting. NORTHCOM also receives reporting from the Central Intelligence Agency (CIA), the FBI, and other agencies through those agencies' working level representatives to NORTHCOM's J2 and CIFC and through senior level representatives that participate in NORTHCOM's Joint Inter-Agency Coordination Group (JIACG).

DoD fully supports the President's initiative to strengthen the analysis and fusion of terrorist-related intelligence and information through the establishment of the Terrorist Threat Integration Center (TTIC). The USD(I) represents DoD's interests within the TTIC, working alongside the CIA, FBI, and DHS. Appropriate DoD intelligence elements, including those from NSA, NIMA, and DIA are contributing their skills and expertise prominently to the TTIC, sharing information and collaborating on analytic products under the direction of the DCI, while still remaining under parent organization authorities. CIFA has a significant role to play, given its unique tools, technology, data exploitation capabilities, and experience in identifying previously unknown or suspected terrorists.

Information sharing with other agencies of the federal government. DoD is working vigorously to promote interagency information sharing. More emphasis is being placed on the need for extensive sharing of both criminal- and intelligence- related information among federal entities and with state and local governments, recognizing that even fragmentary data can help to create a more complete threat picture. There are many examples:

- DIA's Directorate for Human Intelligence continues to dispatch operations officers to FBI Joint Terrorism Task Forces and to DHS Bureau of Immigration and Customs Enforcement facilities to gather information relevant to foreign terrorist threats to the homeland and overseas U.S. military forces. It routinely shares that information with Intelligence Community partners, such as CIA and the State Department's Bureau of Intelligence Research (INR). In addition, DIA is providing DHS with access to all homeland defense-related products, databases, and reports generated or maintained by DIA.

- Foreign threat information collected on U.S. territory by the law enforcement/counterintelligence organizations of the Military Services, and considered to have implications wider than DoD, is pro-actively shared with law enforcement counterparts.
- NSA is collaborating with DHS to incorporate NSA's information superiority products, services, and capabilities that will be responsive to DHS's critical homeland security missions.
- CIFA provides terrorist threat tracking support to a Justice Department effort, with personnel of both organizations working side-by-side.
- The JITF-CT maintains robust connectivity with all Intelligence Community organizations and NORTHCOM.
- The National Reconnaissance Office (NRO) provides a myriad of support to the Department of Homeland Security and law enforcement community. The Deputy Director of National Support/National Support Staff (DDNS/NSS) within the NRO is the customer focal point for external interface with the law enforcement community. Within DDNS/NSS the Homeland Security and Consequence Management Activity is responsible for interface with law enforcement security concerns and crises management. The DDNS/NSS mission relative to law enforcement support is to promote collaboration among civil, defense, and intelligence communities to enhance overall homeland security. The NSS accomplishes this mission by collecting, documenting, and analyzing customer wants and needs; providing education to customers on NRO systems and capabilities; and coordinating operational support to customers. The law enforcement organizations supported by DDNS/NSS include Department of Justice, FBI, Bureau of Immigration and Customs Enforcement, U.S. Marshal Service, Department of Treasury, Secret Service, Alcohol Tobacco and Firearms, Finance Center, Department of Transportation and the U.S. Coast Guard. The NRO established five Law Enforcement Applications Programs based on partnerships between itself, the National Security Agency, and the National Imagery and Mapping Agency.
- The Office of the Inspector General of the Department of Defense, through its Defense Criminal Investigative Service, continues to have a working relationship with the FBI's

> Joint Terrorism Task Forces and the Intelligence Community, thereby fostering the sharing of anti-terrorism information at various levels within Federal and Local Governments. Additionally, the Deputy Inspector General for Inspections and Policy is responsible for implementing and satisfying the Inspector General's statutory duty to "develop policy, monitor and evaluate program performance, and provide guidance with respect to all Department [of Defense] activities relating to criminal investigation programs."

Defense intelligence is being produced at all feasible classification levels in order to serve the broader homeland security community—including personnel who may not have access to secure telecommunications systems. NSA, for example, has implemented a "write-to-release" effort to get information to customers at the lowest possible classification level and to facilitate the further sharing of that information with others who need it but are not directly supported by NSA. Likewise, JITF-CT has developed and implemented a robust automated information sharing capability at the sensitive but unclassified level to facilitate sharing information on suspicious activity and possible surveillance operations among federal, state, and local law enforcement entities. DoD is also supporting the ongoing efforts of the Assistant to the President for Homeland Security, the Information Security Oversight Office, and the Office of Management and Budget to ensure that civil authorities with a need to know obtain security clearances and training in the use, handling, and protection of sensitive and classified homeland security information.

Information sharing during crises often takes place via telephone or video teleconferences, which can occur several times daily during periods of heightened threat. DoD is a charter member of the National Operations and Intelligence Watch Officers Network. DoD routinely activates the network to report the receipt of noteworthy intelligence and to discuss its implications with other federal intelligence watch centers. Additionally, DoD's National Military Command Center controls and frequently convenes Domestic Event Conferences, during which all available information is shared with responsible entities at the federal level during national crises. One of the main problems is the area of communications interoperability along with procedural, cultural, training, and standardization barriers.

Preparation of threat and risk assessments and issuance of warnings. As a partner in the new TTIC, DoD intelligence and investigative elements collaborate with other participating organizations in developing terrorist threat assessments for our national leadership, for the operating forces, and for the DHS. Within DoD, the threat assessment and warning function is managed by the Defense Indications and Warning System (DIWS), comprising defense intelligence elements, Combatant Command indications and warning centers, and national agencies. The DIWS mission is to provide the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other senior U.S. government officials, U.S. military, and allied authorities at all levels with the earliest warning of hostilities or terrorist attacks.

As noted above, JITF-CT is the national-level DoD foreign terrorism intelligence activity that provides threat assessment and warning to support all aspects of DoD's force protection and combating terrorism campaign. The defense agencies, the Military Services, and the Combatant Commands, among others, are responsible for insuring that JITF-CT receives the information,

support, and expertise it needs to carry out this responsibility. A key element of this support emanates from the DoD Force Protection Detachments. Established as a direct result of the COLE Commission findings and under the cognizance of CIFA, these detachments will be located in twenty locations worldwide, where DoD personnel and units regularly transit but where DoD does not maintain a permanent presence.

The NORAD-NORTHCOM CIFC uses a process called Operational Net Assessment (ONA) to synthesize intelligence and information. ONA is a collaborative process involving geospatial overlays, friendly force and critical infrastructure lay down (with Joint Staff input), threat information and assessment, and course of action development. Vulnerability analysis and red teaming are also pieces of ONA. The CIFC provides this fused intelligence and information picture to the NORAD-NORTHCOM Commander, staff, components, and the Operational Intelligence Watch via a variety of means. The CIFC is responsible for many Intelligence and Information functions and includes analysts, liaison officers, and, during crisis or war, combines with the J2 Operational Intelligence Watch to form the Combined Intelligence and Fusion Group. The CIFC also receives "special assessment" input, as required, from subordinate commands, Combatant Commands, and other intelligence centers. National agency representatives, including the FBI and service Counterintelligence/Law Enforcement (CI/LE) personnel, are embedded in the N-NC/J2 and CIFC to facilitate receipt of sensitive CI/LE information and subsequent fusion with traditional sources of intelligence.

The NORAD-NORTHCOM Operational Intelligence Watch provides continuous intelligence to detect and report time-sensitive intelligence information on developments that could involve a threat to the United States. It includes forewarning of enemy actions or intentions, or of imminent hostilities; insurgency, nuclear or non-nuclear attack on the United States, overseas forces or allied nations; hostile reactions to U.S. reconnaissance activities; and terrorist attacks or other similar events.

RELATIONSHIPS WITH NON-DOD ENTITIES

Federal government departments and agencies

DoD interacts on many levels within the interagency community for issues relating to homeland security in order to provide military-unique capabilities. The nature of these relationships ranges from simple communications and situational awareness to on-site liaisons to working side-by-side in an area of operations. Many of these relationships are the result of cooperation outlined in the Federal Response Plan, participation in Military Support to Civil Authorities, critical infrastructure protection activities, and intelligence sharing.

Departments and agencies of the federal government with which DoD has relationships related to homeland security include but are not limited to the Departments of Agriculture, Commerce, Energy, Health and Human Services, Homeland Security, Interior, Justice, State, Transportation, and Veterans Affairs, the Agency for International Development, Environmental Protection Agency, General Services Administration, NASA, National Communications System, Tennessee Valley Authority, U.S. Postal Service, CIA, FBI, and the National Interagency Fire Center.

The Secretary of Defense will work with the Secretary of Homeland Security on policy and resource issues. The ASD(HD) is DoD's primary interface with the DHS. Additionally, NORTHCOM, through the ASD(HD), will work with various components of the DHS on operational planning, training, exercises, and execution.

State and local governments

DoD has a variety of relationships with state and local governments independent of those between state National Guard forces and DoD. Some examples are the following:

- The Military Emergency Preparedness Liaison Officer (EPLO) Program establishes liaison officers and support personnel in each state, with duty at the Governor's respective Department of Military Affairs or State Department of Defense, under the States Adjutant Generals to coordinate mutual DoD support for national security emergency preparedness, response to natural or man-made disasters, and other domestic emergencies.
- Installation commanders support community relations with local governments in order to address local security issues.
- DoD often participates in state-sponsored councils that focus on homeland security issues.

NORTHCOM works with regional and state-level Emergency Preparedness Offices to coordinate capabilities, plans, and operations. NORTHCOM also includes state-level emergency response organizations in training activities and homeland defense exercises.

National Guard and Reserve components

The relationship between the Department, including its combatant commands, and the National Guard and Reserve is the same with respect to homeland security roles as it is in a warfighting context. In cases where the governors of the states and territories employ National Guard forces in a state status to perform state missions of a homeland security nature, those National Guard forces have no direct operational relationship to the Department or its combatant commands. However, the National Guard and Reserve components represent the nation's strategic reserve of organized military capability, and are critical to the Department's ability to sustain long-term military operations.

National Guard personnel serving in a State Active Duty or Title 32 status remain subject to recall to active duty under Title 10 to meet federal requirements. The Chairman, Joint Chiefs of Staff, maintains visibility of National Guard assets performing homeland security missions, as do combatant commanders in order to adjust warfighting plans if necessary to overcome reductions in assigned capabilities. Moreover, NORTHCOM and PACOM must have insight into state-controlled National Guard operations to facilitate coordination between Title 10 and Title 32 or State Active Duty military operations, which might be occurring in the same area, at the same time, towards a common goal.

NORTHCOM has a close relationship with the National Guard Bureau (NGB) of the Departments of the Army and the Air Force, which is enhanced by having a Major General from the Army National Guard as the NORTHCOM Chief of Staff. Through the NGB, NORTHCOM coordinates with state headquarters for planning purposes, and maintains situational awareness of National Guard actions and commitments. The NGB is the channel of communication between the Departments of the Army and the Air Force and the several states on all matters pertaining to the National Guard, the Army National Guard, and the Air National Guard. The Joint Staff and combatant commanders will use the NGB directly or through the Services to gain insight into state-controlled National Guard operations.

The ASD(HD) will develop appropriate policy guidance for DoD Components, including National Guard and Reserve forces, on the employment of forces in support of DoD domestic emergencies and those actions pertaining to homeland defense. In addition, the ASD(HD) will coordinate with the Under Secretary of Defense for Personnel & Readiness on manpower, readiness, medical, and Reserve component matters that impact on homeland defense and DoD support to civil authorities.

The Department continues to define its roles and missions in homeland security in terms of four sets of conditions: those which represent routine sustaining operations and other extraordinary, emergency, or limited scope/duration situations. The mix of forces between the Active and Reserve components ultimately required to meet the Department's worldwide and homeland missions will continue to evolve as emerging requirements are defined, yet the Department foresees no significant changes affecting the Guard and Reserve.

CURRENT & PROJECTED DOD RESPONSE CAPABILITIES–CBRNE

All commanders have the responsibility to assess their installations and facilities for vulnerabilities to threats, to include CBRNE hazards, and to reduce their vulnerability to these threats within the scope of available resources and in priority to the perceived threat. Over the past decade, the focus of force protection has been toward high explosives and cyberterrorism. While CBRN hazards have been identified as a potential threat, the judgment of most installation commanders is that the likelihood of an actual CBRN incident is much less than a "conventional" terrorist incident. The anthrax letter attacks of 2001 and subsequent evidence of Al Qaida's pursuit of CBRN capabilities have increased appreciation for the growing CBRN threat to DoD installations and facilities.

All installations with force protection programs have assessed their vulnerabilities to CBRNE hazards and have taken aggressive steps to monitor and deter such incidents. They have identified the vulnerabilities present and what steps are necessary to address these vulnerabilities. However, because conventional terrorist threats have been seen as more credible and therefore a higher priority, resources to address potential CBRNE terrorist incidents have been minimal. As a result, the actual capability to protect personnel on these installations and to respond to such an event is extremely limited, especially on installations in the continental U.S. One of the limiting factors that has delayed the implementation of protective measures has been the lack of a DoD policy on chemical-biological (CB) protection of civilians. The Deputy Secretary of Defense issued policy on this subject on September 5, 2002 and the Chairman of the Joint Chiefs of Staff

is in the process of developing recommendations on how to implement this policy. The implementation policy is expected to be completed not later than October 2003.

Until recently, another limiting factor was the lack of DoD-wide guidelines for developing an organic emergency response capability for CBRNE hazards. This factor has been addressed with the release of DoD Instruction 2000.18, "DoD Installation CBRNE Emergency Response Guidelines," in December 2002. Emergency responders, while having some training and equipment for hazardous materials (to include toxic inhalation hazards and radiological contamination), have had limited capability with respect to more toxic chemical warfare agents and biological organisms.

Following the September 11, 2001 attacks, the Department convened a number of working bodies to address the vulnerability of DoD installations and facilities to CBRNE hazards in an effort to develop a comprehensive plan to improve the preparedness of these installations against the effects of CBRNE incidents. Initial proposals to use military sensors, protective equipment, and decontamination applicators across all installations identified a potentially large investment and annual sustainment costs that were not acceptable.

Therefore, to better identify the exact capabilities required at DoD installations and facilities, the Department initiated a Joint Service Installation Pilot Project (JSIPP), which is being executed during FY03. JSIPP is fielding a number of CB sensors and associated equipment at nine DoD installations (three Army, three Air Force, two Navy, one Marine Corps), outfitting their installation emergency responders with appropriate response equipment, refining concepts of operation, and evaluating the installations' increased capability to respond to CBRNE incidents. The JSIPP does not include protective equipment, medical countermeasures, or decontamination capabilities for the DoD civilians on the installation. The results of the JSIPP will be available in the first quarter of FY04.

Based on the results of JSIPP and other ongoing installation protection efforts, the Department will initiate a larger scale effort to outfit 200 DoD installations with CBRNE defense capabilities between FY04 and FY09. The Department is in the process of identifying the specific installations, based on the critical nature of the installations' mission and population. Funds have been identified, based on the current JSIPP model, to outfit these installations with CB defense capabilities and their installation emergency responders with appropriate response equipment. The Services and Defense agencies will sustain this capability with operations and maintenance funds identified for this purpose.

The Department is developing a capabilities-based approach to address the remaining installations and facilities. One of the constraints is the need to develop a flexible strategy that takes into account that not all installations have an inherent emergency response capability, nor can they afford to sustain a large number of CB sensors, radiological, and other support equipment. There are, however, other steps such as employee education and protective measures that can be taken in the event of a CBRNE incident. The Department anticipates the development of a tiered approach to provide equipment and concepts of operation to larger installations and facilities. These larger units have a critical warfighting mission and host inherent emergency response capabilities. Smaller and less critical installations and facilities

have a more limited suite of capabilities that is both sustainable and justifiable in light of their mission and population.

Another key element of this effort is the coordination of local, state, and federal response elements outside of these installations and facilities. Consequence management operations are a key element in all force protection programs and, as such, all installation commanders are required to develop these plans. In many cases, installations have already developed mutual aid agreements with the local and state emergency responders. Ensuring that local, state, and federal emergency responders have an adequate capability to assist installations and facilities in responding to CBRNE terrorist incidents will require coordination with the National Guard, Department of Justice, DHS, and NORTHCOM. NORTHCOM commands Joint Task Force-Civil Support, which is charged with maintaining expertise in responding to CBRNE incidents.

Additionally, DoD Directive 6200.3, "Emergency Health Powers on Military Installations" (May 2003), affords installation commanders the authority to take protective measures on DoD facilities and for DoD military, civilian, and contractor personnel in the event of a CBRNE incident.

To ensure that there is a coordinated effort across DoD, the Joint Staff is facilitating an effort to align all installation CBRNE defense protection efforts under an integrated activity, which will be overseen by a general officer/flag officer-level planning team. The team will include the Services, Joint Staff, and elements of the Office of the Secretary of Defense. The efforts to be combined include JSIPP, the 200 installation effort, the response to Deputy Secretary's memorandum dated September 5, 2002, the requirement for a biological weapons defense concept of operations, the Defense Threat Reduction Agency's Unconventional Nuclear Weapons Defense effort, and other ongoing force protection efforts involving the equipping of emergency responders with CBRNE defense equipment.

Biological Defense Research programs

In accordance with public law (50 USC 1522), CB defense research is conducted under the DoD Chemical and Biological Defense Program (CBDP). This research is overseen by a single office within the Office of the Secretary of Defense: the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB)). Biological defense research is conducted in support of operational missions of the U.S. military. While it does not directly support homeland security, the results of the research and the infrastructure are frequently leveraged to enhance the research efforts of lead federal agencies. Detailed information on DoD biological defense research is also available in the *Department of Defense Chemical and Biological Defense Program Annual Report to Congress*.

Biological defense research is directed to the discovery, evaluation, and exploitation of technology to address the threat of biological weapons and to ensure the safety and mission effectiveness of U.S. forces operating within a contaminated environment with minimal impact on logistics. Biological defense research is organized into research areas that support the Joint Future Operational Capabilities and includes detection, information technology, protection, medical biological defense, and decontamination.

The CBDP coordinates efforts with other U.S. government agencies and with other countries to ensure that the DoD has a world-class chemical and biological defense capability that addresses all current and future threats to warfighter and homeland security missions. For example, the Chemical and Biological National Security Program, formerly in the Department of Energy and now an element of the Department of Homeland Security, coordinates technology development efforts with DoD through the development of technology roadmaps.

Similar coordination is being developed with the National Institutes of Health (NIH). Following the terrorist attacks of September 11, 2001 and the anthrax letter attacks of late 2001, Congress appropriated approximately $1.7 billion for a Counterbioterrorism Research Program to be managed by the National Institute of Allergies and Infectious Diseases (NIAID). However, NIAID has only a modest research investment in this area while the DoD Medical Biological Defense Research Program (MBDRP) has the infrastructure and expertise necessary to support this effort. Furthermore, NIAID's published strategic plan overlaps significantly with the MBDRP. To prevent unnecessary redundancy, the NIAID and the U.S. Army Research Institute of Infectious Diseases—the MBDRP lead laboratory—entered into an agreement to coordinate portions of their biodefense research and development programs including a shared animal facility, cooperative development of vaccines, drugs, alternate therapies and diagnostics, and development of standardized strain collections.

An example of a biological defense research effort that is aimed directly in support of the homeland security mission is the Multimission Sensor (MMS) Program. The MMS program uses existing radars (e.g., Doppler weather radars) to provide early warning of a suspected chemical or biological (CB) event to allow timely dispatch of a dedicated CB sensor to confirm or deny the existence of the CB event.

In addition to the biological defense research efforts conducted under the CBDP, the Defense Advanced Research Projects Agency (DARPA) manages a Biological Warfare (BW) Defense Program. In coordination with the CBDP, DARPA seeks breakthrough concepts and technologies that will enhance our national security. DARPA's BW Defense Program is intended to complement the DoD CBDP by anticipating threats and developing novel defenses against them. The DARPA program is unique in that its focus is on the development of technologies with broad applicability against *classes* of threats. DARPA invests primarily in the early technology development phases of programs and the demonstration of prototype systems. Below is a selected list of ongoing DARPA biodefense research efforts related to sensors, protection, and medical countermeasures.

- Sensors
  - The BW Defense Environmental Sensors Program develops technologies to enable bioagent detection and identification.
  - The Activity Detection Technologies Program explores the development of activity detection systems, which report on functional consequences of exposure (mechanism and activity) to a wide spectrum of chemical or biological toxins which may have been bioengineered and are currently undetectable by other means.

    - The Pathogen Genome Sequencing Program is sequencing genomes of BW threat agents to establish a basis for low false alarm detection and identification.
- Protection
    - Air purification systems are under development to (1) provide filtration media with lower pressure drops, greater capacity, improved retention, and possible neutralization of the pathogens, (2) destroy and neutralize chemical and/or biological agents using a small catalytic oxidation reactor, and (3) provide advanced low-cost filters designed and packaged for the next generation of a joint service mask and masks designed for first responders.
    - Water purification systems are under development using innovative approaches to disinfect and purify water from any source in the field.
    - Decontamination and neutralization methods are under development for destroying agents in a non-corrosive manner without using extremely high power or harmful chemicals. Current methods employ concentrated bleach that can be corrosive or methods that use extremely high power lasers, lamps, or discharges.
    - The Immune Building Program is developing technologies and systems to allow military buildings to respond actively to attacks by chemical or biological agents so as to (1) protect human occupants from the lethal effects of the agent, (2) restore the building to function quickly after the attack, and (3) preserve forensic evidence about the attack. These technologies will greatly reduce the effectiveness of attacks and make the buildings less attractive as targets.
- Medical
    - DARPA is pursuing the development and demonstration of capabilities for real-time environmental sensing; medical countermeasures (barriers to the entry and spread of pathogens); and advanced medical diagnostics for the most virulent pathogens.

Need for and feasibility of developing and fielding regional DoD chemical-biological incident response teams

The DoD response to a domestic CBRNE incident will be in support of civilian authorities unless it is on a military installation. The Federal Response Plan states, "DoD will normally provide support only when other resources are unavailable, and only if such support does not interfere with its primary mission or ability to respond to operational contingencies."

For the past two years the Department of Justice and FEMA have been conducting assessments on the need for additional CB incident response capability. These agencies, led by the Department of Homeland Security and with support from DoD, should be the requirements developers, taking into consideration the capabilities already in place in the various federal, state, and local emergency response agencies.

DoD's part in an assessment of this type should be to 1) evaluate the total DoD force structure for appropriate capabilities and identify any gaps that may exist, and 2) determine the requirements to field additional structure to fill these gaps. Basic capabilities include:

1. Agent detection/identification
2. Chemical/biological sampling

3. Hazard area identification/prediction
4. Personnel/equipment decontamination
5. Triage and emergency medical treatment
6. Epidemiological investigation
7. Site security
8. Evacuation/rescue

There are several types of units that could be mobilized (or placed on state active duty, in the case of the National Guard) to provide these capabilities. The DoD has established 32 WMD-CSTs that can perform the first three tasks listed above and assist or advise the Incident Commander regarding the other tasks. These teams are dedicated to domestic operations.

The Department does not support creation of regional military chemical-biological incident response teams. It is envisioned that civilian responders will arrive on the scene of a domestic incident in advance of the military and therefore will be able to mitigate loss of life and property damage to a far greater extent than any later-arriving DoD response forces. In coordination with DHS, DoD is prepared to assist in the development and training of regional CBRN response capabilities within the civilian sector. This transfer of capabilities to the civilian sector would benefit from DoD's past experience related to both operational concepts and CBRN technology.

CURRENT AND PROJECTED DOD RESPONSE CAPABILITIES– CYBERTERRORISM

Current efforts

Within the Department of Defense, almost all information assurance spending ($2 billion in FY03) addresses cyberterrorism in that it is used to protect and defend our networks against attack. These efforts prepare DoD to defend against hackers, criminals, and other nations as well as cyber-terrorists. Therefore, there are no elements of information assurance funding specifically targeted at cyber terrorism.

The ASD(SO/LIC) is responsible for the management and technical oversight of the Technical Support Working Group (TSWG), an interagency working group that addresses technology development issues with regard to combating terrorism. Its Infrastructure Protection subgroup reviews and makes recommendations on two overarching aspects of the infrastructure assurance problem: the cyber security aspect and the impact of cyber attacks on physical assets. Within the DoD, Strategic Command has forces designated to defend against cyberterrorism, specifically, the Joint Task Force-Computer Network Operations and the Joint Information Operations Center.

Developmental programs

Cyber security projects focus on preventing or mitigating threats to computer networks vital to defense. The complexity and sophistication of information technologies and widespread integration in other infrastructures increases the likelihood of unforeseen vulnerabilities. Current

research will provide detection, prevention, response, and alert capabilities to counter attacks and harden computer systems.

The following TSWG Infrastructure Protection projects total about $1.7 million in FY02 and a planned $2.3 million in FY 03:

- The Electric Power Infrastructure Database will be an unclassified, geo-referenced electric power generation and transmission database that will support hazard prediction, damage estimation, and consequences assessment with respect to the broad range of natural and technological disasters and threats.
- The Hacker Site Replication Tool provides a resource for intelligence and law enforcement personnel to capture suspect web site content, archive it off-line, and perform in-depth forensic searches on servers removed from the Internet. This approach provides near real-time currency of data without unduly alerting the interest of web site personnel.
- The Flash Read-Only Memory Vulnerability Countermeasure Toolkit will characterize, monitor, protect, and if necessary, repair Flash ROM contents. This will prevent the insertion of programs into computers and networks by unauthorized users.
- The Secure Teleconferencing Bridge will allow government organizations to communicate with multiple parties simultaneously in a secure, but unclassified environment. The secure bridge will send encrypted communications to as many as 30 connected devices, both fixed and mobile.
- The T-LAN Analyzer project will develop a system that can detect, record, and block unauthorized traffic entering or leaving a secure facility via the local area network systems. Unauthorized traffic will trigger an alarm and will be flagged, recorded, and/or blocked based on a predetermined set of processing algorithms.
- The Systems Administrator Simulation Trainer will be an environment for system administrators to learn how to apply a broad range of defensive technologies and strategies, providing high-fidelity experience in resisting, responding to, and recovering from cyber attacks.
- The Alert Trend Change Detection Tool will be the next-generation probe detection tool for the Federal Aviation Administration. It will analyze entry port scans and probe alerts, looking for patterns that indicate attacks by malicious agents. The tool warns security analysts monitoring the network and provides alert trend information in several formats.
- The Communications Firewall will recognize, record, and/or block unwanted signals entering or leaving a Sensitive Compartmented Information Facility via telephone circuitry. Eventually, the capability can be extended to other signals such as local and wide area networks, cable TV, video, and classified circuits (secure switched communications, secure networks, etc.). This task is a collaborative effort with the Air Force.

PREPARATION AND TRAINING FOR DOD'S HOMELAND DEFENSE AND CIVIL SUPPORT ROLE

Training and education for homeland defense and civil support missions

NORTHCOM is establishing a robust education and training program in cooperation with other DoD components and other agencies. It is also working closely with the National Defense University, the Naval Postgraduate School, and the University of Colorado in Colorado Springs in the development of a Masters Degree Program in Homeland Security. NORTHCOM will cooperate with DHS through the Office of Domestic Preparedness in further developing homeland security training.

NORTHCOM coordinates its exercise schedule with NORAD, Cheyenne Mountain Operations Center, PACOM, STRATCOM, and the interagency. NORTHCOM executes two major exercises each year: UNIFIED DEFENSE in the spring and DETERMINED PROMISE in late summer. The focus of each exercise is on crisis and consequence management with the employment of a Joint Task Force. NORTHCOM's supporting operational plan for a concurrent major theater war outside the United States is also exercised.

The Defense Threat Reduction Agency's (DTRA) Defense Nuclear Weapons School (DNWS), located at Kirtland Air Force Base, New Mexico, creates, develops, and implements professional training in special weapons competencies for the DoD to ensure that armed forces and emergency response personnel are prepared to meet critical Weapons of Mass Destruction (WMD) national defense challenges of the future. Resident courses and mobile training subjects include, but are not limited to, radiological emergency team operations, WMD planning and command and control, and nuclear surety. DNWS also maintains a mobile training team capable of delivering training to audiences throughout the country such as National Guard WMD Civil Support Teams.

DTRA has been given responsibility for the conduct of combatant commander-level consequence management exercises in concert with the Department of State. By providing technical and operational experience and expertise gathered from supporting similar exercises in the continental United States, DTRA aids combatant commanders and overseas personnel in the development of consequence management plans.

DTRA maintains several rapidly deployable Consequence Management Advisory Teams (CMATs) that have specialized expertise to support DoD elements that oversee CBRNE consequence management and planning. Through direct liaison with the geographic combatant commands and other federal agencies, participation in exercises, and coordinated deliberate planning, the teams have the capability to deploy and rapidly augment the theater Crisis Action Teams and other emergency response organizations in the event of a CBRNE event. CMATs regularly deploy to the FBI's Strategic Information Operations Center in preparation for National Security Special Events such as presidential inaugurations.

Integrated training with non-DoD entities

NORTHCOM is working with federal, state, and local agencies to nominate the DETERMINED PROMISE exercise in even-numbered years as the major interagency exercise for that year, starting in FY04. In the alternate years, the major interagency exercise will be the TOP OFFICIALS (TOPOFF) exercises.

DTRA provides critical support in several domestic real-world missions and training exercises. First, as DoD's Executive Agent for Nuclear Weapons Accident Exercises, DTRA coordinates with FEMA, the FBI, and a number of other federal, state, and local authorities to prepare for emergency operations in response to an accident involving nuclear weapons. DTRA also supports exercises such as TOPOFF and real world events such as presidential inaugurations.

DTRA conducts vulnerability assessments to benefit the DoD and non-DoD federal executive branch departments and agencies. It also performs vulnerability assessments on sites or facilities nominated by the National Guard of the individual states. Balanced Survivability Assessments provide decision-makers with a comprehensive vulnerability analysis that demonstrates the vulnerabilities of critical national mission architectures, systems, nodes, and infrastructures and provides essential vulnerability information and recommendations for mitigation. This methodology has been applied extensively to assist non-DoD executive branch departments and agencies, such as FEMA, the Department of Health and Human Services, the U.S. Coast Guard, and the Department of State. Special assessment support has also been provided to Congress (U.S. Capitol and associated office buildings), the North Atlantic Treaty Organization, and selected allied governments.

Joint Staff Integrated Vulnerability Assessments (JSIVAs) are conducted for DoD fixed sites, airports, seaports, and headquarters facilities. Assessed installations and organizations also receive follow up assistance to help train assessment teams to conduct tailored assessments and to provide other specialized assistance as required. Vulnerability trends, anti-terrorism (AT) lessons learned, and AT best practices are provided to the Joint Staff. JSIVAs have also been conducted for non-DoD sites such as the U.S. Capitol and one of the U.S. Senate buildings.

Finally, the DoD Critical Infrastructure Protection (CIP) program focuses on the identification, assessment, and security enhancement of physical and cyber assets and associated infrastructures essential to the execution of the National Military Strategy. Multiple activities within DoD conduct CIP vulnerability assessments at varying levels of fidelity, including the U.S. Transportation Command, the Defense Logistics Agency, the U.S. Army Corps of Engineers, DTRA, the Defense Information Systems Agency, and the Joint Project Office for Special Technology Counter Measures. The sharing and use of vulnerability assessment information among DoD activities is essential to the protection of resources around the world used in support of DoD. While some of these assessments have been conducted for non-DoD sites, including National Special Security Events, the information gathered and maintained by the DoD CIP program has direct applicability to the broader homeland security environment.

Simulations and "red teaming"

NORAD-NORTHCOM's CIFC has begun developing an in-house Red Team as part of its operational net assessment process. This organization will help simulate the planning of terrorists and help answer the questions of how to better protect ourselves. NORTHCOM commenced Red Team training in May 2003 for its CIFC analysts in coordination with the Central Intelligence Agency. Together with the reserve Red-teaming initiatives at Ft. Leavenworth, Kansas, the CIFC will use information from classified and open sources, thus providing a more robust analytical capability for the Command.

FUNDING AND STATUTORY LIMITATIONS

The homeland defense activities and initiatives supporting civilian authorities discussed in this report are all funded in the President's budget. Furthermore, the Department sees no legal impediments to the performance of these activities.

ANNEX

FY 2003 BOB STUMP NATIONAL DEFENSE AUTHORIZATION ACT (NDAA) HOMELAND SECURITY CONGRESSIONAL REPORTING REQUIREMENTS Public Law 107-314, Section 1404

SEC. 1404. REPORT ON THE ROLE OF THE DEPARTMENT OF DEFENSE IN SUPPORTING HOMELAND SECURITY.

(a) **REPORT REQUIRED**.--Not later than March 1, 2003, the Secretary of Defense shall submit to the congressional defense committees a report on Department of Defense responsibilities, mission, and plans for military support of homeland security.

(b) **CONTENTS OF REPORT**.--The report shall include, at a minimum, a discussion of the following:

(1) The Department of Defense definition of its homeland security mission, particularly with respect to how it relates to providing military support to civil authorities, managing the consequences of terrorist attacks, and homeland defense, and the actions the Department is taking to implement the homeland security mission as so defined.

(2) Changes in the roles, missions, responsibilities, organization, and capabilities of the following organizations in order to conduct their homeland security support mission, and the reasons for such changes:

(A) The Office of the Secretary of Defense.
(B) The Army, Navy, Air Force, and Marine Corps.
(C) The Army National Guard and the Air National Guard.
(D) The combatant commands of the Department of Defense.

(3) The relationship between the Department of Defense, including its combatant commands, and the following with regard to homeland security:

(A) Other departments and agencies of the Federal Government.
(B) State and local governments.
(C) The National Guard and Reserve components.

(4) The current capability of the Department of Defense to respond to terrorist attacks employing chemical, biological, radiological, nuclear, high explosive or cyberterrorism weapons against personnel and critical infrastructure of the Department, including identification of the goals of the Department for being fully capable of responding to such attacks, current deficiencies in that capability, the resources required to achieve that capability, and a long-term plan to reach that capability.

(5) The roles, missions, and responsibilities of the intelligence components of the Department of Defense in support of its homeland security mission, including the policies and plans for—

(A) collecting and analyzing information related to homeland security;
(B) sharing that information with other agencies of the Federal Government; and

(C) preparing threat and risk assessments and issuing warnings.

(6) A discussion of plans of the Department of Defense for training, exercising, and preparing to perform its homeland security mission, including--

(A) individual and collective training for civilian and military personnel of the Department involved in homeland security;

(B) integrated training with other agencies of the Federal Government, and with State and local governments, as appropriate;

(C) interagency exercises and simulations; and

(D) the development of a permanent ``terrorist opposing force'' capable of challenging the Department's plans, policies, and capabilities during training events and exercises.

(7) A discussion of how the Department of Defense biological defense research program supports its homeland security mission.

(8) A discussion of the efforts by the Department of Defense to develop, either within the Department or through contracts with private entities, anticyberterrorism technology, including an assessment of whether and how such efforts should be increased.

(9) An assessment of the need for and feasibility of developing and fielding Department of Defense regional chemical-biological incident response teams across the United States, including options for providing the resources and personnel necessary for developing and fielding any such teams.

(10) A discussion of the Department of Defense plans and efforts to place new emphasis on the unique operational demands associated with homeland security while ensuring that defense of the United States remains the primary mission of the Department of Defense.

(11) The resource constraints and legal impediments to implementing any of the activities discussed under paragraphs (1) through (10).