

~~SECRET//NOFORN~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX A TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM (U)

INTELLIGENCE (U)

1. (U) Situation

a. (U) Terrorist Organizations. Terrorist organizations, especially those that have global reach, may be sponsored by states or state-like entities and can instigate direct action from locations worldwide. They operate within a network of decentralized small groups and individuals, minimal infrastructure, and redundant communications which are difficult to locate, target, and attack with direct US and/or coalition military action. The United States must be prepared to preempt or engage terrorists on little notice and be ready to neutralize the infrastructure and enablers that perpetuate or support terrorist organizations (See Appendix 2 to this Annex).

b. (U) State Sponsors. The Department of State designates seven countries as state sponsors of terrorism: Cuba, Iran, Iraq, Libya, DPRK, Sudan, and Syria. State support can take many different forms - regimes that continue to provide material support to terrorist groups are the most active and dangerous of these states. Additionally, all of the countries on the Department of State list maintain chemical and/or biological warfare programs (See Appendix 3 to this Annex).

(b)(1)



~~CLASSIFICATION~~
~~EXCLUDED FROM AUTOMATIC DOWNGRADING AND DECLASSIFICATION~~
~~EXCLUDED FROM AUTOMATIC DOWNGRADING AND DECLASSIFICATION~~
~~EXCLUDED FROM AUTOMATIC DOWNGRADING AND DECLASSIFICATION~~

~~SECRET//NOFORN~~

2. (U) Nature of the Threat. Terrorist networks operate from widely dispersed locations and offer few critical nodes to attack. These adversaries are adaptive and clever – identifying and exploiting US vulnerabilities. The most likely threat to US personnel, organizations, or facilities are radical terrorist organizations identified in the Threat Matrix (Appendix 1 to this Annex). Four criteria distinguish these organizations:

a. (U) Capability and Intent for Mass Casualty Attacks. Organization possesses weapons to inflict multiple casualties against US personnel and may have access to weapons of mass destruction including CBRN weapons.

b. (U) Anti-US Intentions. Most resources are dedicated to attacks on US interests. Group has a history of executing or planning anti-US attacks.

c. (U) Operational Sophistication. Organization possesses capability to plan, resource, and execute an attack on the United States and its interests.

d. (U) Global Reach. Organization has operational and support network in multiple countries and possesses the capability to recruit, plan, resource and execute terrorist attacks worldwide including within the US homeland.

(b)(1)



4. (U) Critical Capabilities. Destroying and defeating transnational terrorist networks requires comprehensively attacking the critical capabilities terrorists depend on for global action. Terrorist organizations with religious, political or economic motivation may have different sources of strength, capabilities, and vulnerabilities, which will dictate US ways and means of attack. Five capabilities are essential to all known terrorist groups:

a. (U) Generation of Manpower and Ideology. It is the terrorist's unique ability to recruit and influence individuals to commit extraordinary, horrific

and often self-destructive acts, all on behalf of simple ideas independent of the nation-state, that separates them from virtually every opponent US forces have faced before. The principal source of strength for networks like al-Qaida is the ideological appeal and perceived religious legitimacy used to recruit and retain a significant and globally dispersed constituency. This source of strength is difficult to attack militarily.

b. (U) Command, Control, and Communications. Terrorist organizations rely on networks made up of composite cells to plan, organize, and communicate. Terrorist organizations with global reach rapidly adapt their planning and execution to fit specific operations. These capabilities are enhanced when operating under the cover of state sponsored sanctuary or sanctuary in ungoverned space.

c. (U) Funding. Terrorist networks may operate autonomously or enter into relationships with state or nonstate entities that are willing to sponsor their activities, as well as provide material and financial support – including access to dangerous technologies. Such relationships can dramatically expand the terrorist's capability to conduct more effective and deadly operations. Terrorists must raise money or access funds required to underwrite their activities. They rely on funds that are often dispersed internationally, harbored within nongovernmental organizations (NGOs), licit and illicit financial institutions, and the institutions of state sponsors. Terrorist groups often use illicit means of generating funds such as illegal drug trade, kidnapping, and extortion.

(b)(1)



e. (U) Sanctuary. Sanctuary is the terrorist's most important asset. The more secure the sanctuary, the more likely the terrorist can operate with impunity. The transnational terrorist increasingly leverages the geographic sanctuary of ungoverned space or state sponsorship; the legal sanctuaries afforded by the rules and rights of free and open societies; and the anonymity, influence, and reach extended to individuals and small groups by increasing globalization. The existence and utilization of ungoverned and under-governed space largely enable the most immediate terrorist threats. Defeating these threats requires increased efforts to reduce and eliminate the advantage these spaces afford.

5. (U) Concept of Intelligence Operations. Combating terrorism requires innovative and responsive approaches to intelligence collection and dissemination processes. The global reach of terrorism demands close synchronization and integration among geographic and functional capabilities of US and allied and/or coalition intelligence to allow the United States to attack these individuals and organizations before they can take defensive actions or further offensive actions.

a. (U) National Intelligence. Under the Director of Central Intelligence, the US intelligence community has focused and coordinated efforts to counter terrorism and terrorists in all forms. That coordination extends to the DOD intelligence organizations and efforts.

b. (U) DOD Intelligence. The Director, Defense Intelligence Agency (DR/DIA), oversees the coordination of defense intelligence requirements to ensure intelligence support is provided to the Department of Defense. When necessary, the DR/DIA will convene the Military Intelligence Board (MIB) to serve as the senior "Board of Governors" for the DOD Intelligence Community. The MIB serves as a forum for discussion of intelligence requirements and support provided by the DOD intelligence components. Specific MIB responsibilities include coordinating intelligence support to military operations; serving as a forum for discussion and development of coordinated positions on community substantive and resource issues; and providing oversight and direction to defense intelligence production, collection, and infrastructure. Crisis MIBs are normally convened in response to an imminent or ongoing crisis. The crisis topic may involve a geographic (i.e., Afghanistan), functional (i.e., terrorist bombings in East Africa), or systemic crisis (i.e., HLS).

c. (U) Joint Intelligence Task Force - Combating Terrorism (JITF-CT). The JITF-CT has been established as a consolidated DOD all-source intelligence fusion center that is staffed, equipped, and empowered to support an aggressive, worldwide campaign against terrorism.

(1) (U) The JITF-CT will support the full range of DOD efforts to combat terrorism, both offensive and defensive, with focus on providing strategic and tactical warning, exposing and exploiting terrorist vulnerabilities, and providing timely intelligence to prevent terrorists and their sponsors from acquiring increased capabilities, particularly in the area of WMD.

(2) (U) The JITF-CT will integrate national-level analytic efforts to meet DOD intelligence requirements. At the national level, JITF-CT will be an inject point for non-DOD intelligence and domestic law enforcement agencies to integrate terrorist data and conduct initial coordination and collaboration with DOD entities. JITF-CT will produce all-source, tailored intelligence supporting

DOD CT and antiterrorism operations, planning, and policy. The JITF-CT is an all-source analytic organization; therefore, complete access to the full range of all-source intelligence reporting, including counterintelligence information will be a key enabler to this process. Cooperation among the Intelligence Community organizations and the law enforcement community to ensure transparent sharing of information will be the key to the JITF-CT mission.

(3) (U) DR/DIA has assigned the JITF-CT to the Joint Staff Intelligence Directorate (J-2), the national level focal point for indications and warning (I&W), crisis support, and current intelligence support to military operations and combatant commanders' intelligence requirements. Theater intelligence centers will continue to interface directly with the JITF-CT on terrorism-related issues as necessary.

d. (U) Crisis Intelligence Federation. Combatant commanders will develop, with the assistance of Joint Staff J-2 and in accordance with the Crisis Intelligence Federation CONOPS, intelligence federation partnerships in direct support to theater CT campaign plans. Federation CONOPS will identify intelligence support functions that will be federated to partner combatant commanders, Services intelligence centers, combat support agencies, and national intelligence agencies. Joint Staff J-2 will validate and prioritize all requests for federated support.

e. (U) Quick Reaction Team (QRT). Combatant commanders will identify requirements for the deployment of the USJFCOM-based QRT to supplement theater targeting and collection management personnel during theater CT campaign plan execution. Coordinate QRT deployment with Joint Staff J-2 and USJFCOM in accordance with the QRT CONOPS.

f. (U) Augmentation. Requirements for individual augmentation will be requested in accordance with the CJCSI 1301.01B process.

g. (U) National Intelligence Support Team (NIST). All combatant commander's-validated requests for national intelligence support, including NIST requests, should be sent to Joint Staff J-2 for approval. Requests should include clearly delineated intelligence requirements so that support can be tailored to meet the needs of the JTF or supported command.

(b)(1)



i. (U) Foreign Disclosure and Release Policy. Sharing US military intelligence – while protecting sources and methods – will remain one of the keys to sustaining multinational force operations. However, it is not possible to establish a single foreign disclosure and release policy scenario for all multinational operations. Each coalition or alliance will require the development of its own procedures unique to the situation.

6. (U) Priority Information Requirements

(b)(1)



~~SECRET//NOFORN~~

(b)(1)



(b)(1)

a. (U) Elements of a Long-Term Intelligence Collection Strategy

(b)(1)



~~SECRET//NOFORN~~

(b)(1)

(b)(1)



(b)(1)

d. (U) ISR Allocation. In order to ensure the most efficient and rational allocation of collection resources, all OPLANs from combatant commanders must include, in Annex B, a detailed list of priority intelligence requirements and subordinate essential elements of information (EEI) as the basis for collection requirements. Combatant commanders will craft collection requirements to address these EEI, documenting these requirements in accordance with DOD collection management procedures for HUMINT, counterintelligence (CI), imagery intelligence, signals intelligence, measurement and signatures intelligence, open source intelligence, and airborne ISR. The Joint Staff will use these requirements to make allocation decisions, especially for low density/high demand (LD/HD) resources such as airborne ISR platforms. Our airborne allocation tool will provide a baseline for combatant commanders to develop airborne situation assumptions in their collection plans. Combatant commanders' Annex Bs will also include a comprehensive ISR CONOPS – fully integrated with the combatant commanders campaign plan – that links the specific information requirements that need to be satisfied to the requested ISR systems' capabilities and tasking, processing, exploitation and dissemination architecture.

(b)(1)



(b)(1)



c. (U) Time-Sensitive Targets (TST). For some critical, time-sensitive types of targets, the time available to acquire, target, and attack may be very brief. In these cases, an accelerated targeting cycle must be used where all phases take place simultaneously or on a compressed time line. TSTs are those targets requiring immediate response because they pose (or will soon pose) a danger to friendly forces or are highly lucrative perishable targets of opportunity. TSTs are high payoff targets or may be engaged to deter aggression or the use of force against US interests.

(b)(1)



9. (U) Processing, Exploitation, and Dissemination

a. (U) Intelligence Systems Architecture. The joint intelligence architecture encompasses collection, processing, exploitation, and dissemination nodes. These nodes are supported by a robust communications infrastructure and automated systems equipped with tailored applications to meet the broad array of intelligence activities supporting joint military operations. Command, Service, and agency intelligence processes ride on a communications backbone of Joint Worldwide Intelligence Communications System, and the Secret Internet Protocol Router Network. This infrastructure is supplemented by a distributed, common exploitation and dissemination system, tactical data links, and intelligence broadcast services.

b. (U) Global Command and Control System. The Joint GCCS serves as the primary C4I system for the Joint Force Commander, using Integrated Imagery and Intelligence (GCCS-I3) applications to provide a standard set of integrated, linked tools and services that give ready access to imagery and intelligence directly from the commander's common operational picture (COP). The GCCS is complemented by Service C4I systems (GCCS-Maritime, GCCS-Army/All-Source Analysis System, Theater Battle Management Core System, Intelligence Analysis System), the Joint Deployable Intelligence Support System, and a variety of DOD Intelligence Information Systems and mission applications. GCCS-I3, available at both the collateral and SCI levels,

enhances the COP by providing a standard set of integrated, linked tools and services that give ready access to imagery and intelligence seamlessly plotted on the COP. GCCS-I3 establishes a common, accurate, and shared intelligence reference data baseline for joint mission planning, execution, and assessment, enabling commanders and staffs.

c. (U) Collection Management Systems. Upon fielding the Collection Management Mission Applications (CMMA), combatant commands, Services, and agencies will fully integrate it into their collection management CONOPS. CMMA will provide vital ISR operational data, enabling commanders and staffs to recognize gaps and opportunities that directly support operations.

10. (U) Counterintelligence

(b)(1)



~~SECRET//NOFORN~~

(b)(1)



Appendixes

- 1 -- Terrorist Threat Matrix
- 2 -- Terrorist Organizations
- 3 -- State Sponsors
- 4 -- Weapons-of-Mass-Destruction (WMD) Terrorism
- 5 -- Interrogations

~~SECRET//NOFORN~~

(b)(1)

(b)(1)



(b)(1)



(b)(1)



(b)(1)

(b)(1)

(b)(1)

(b)(1)

(b)(1)



~~SECRET//REL TO USA, AUS, CAN AND GBR//X1~~

INTENTIONALLY BLANK

~~SECRET//REL TO USA, AUS, CAN AND GBR//X1~~

APPENDIX 1 TO ANNEX A - TERRORIST THREAT MATRIX

A-1-10

~~SECRET~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 2 TO ANNEX A TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

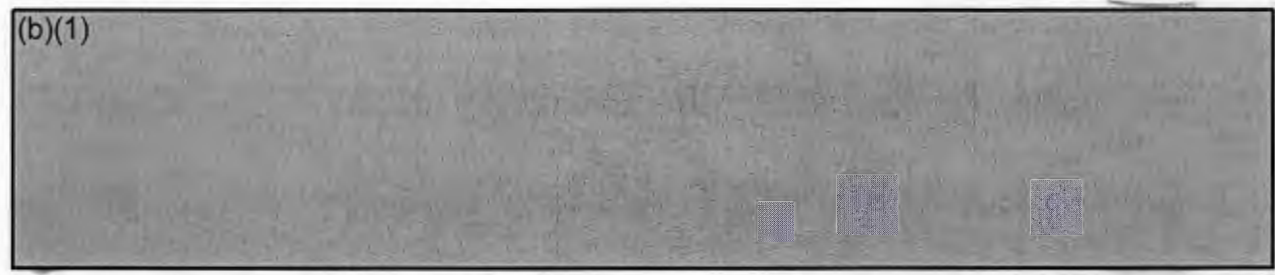
TERRORIST ORGANIZATIONS (U)

(b)(1)



1. (U) Al-Qaida

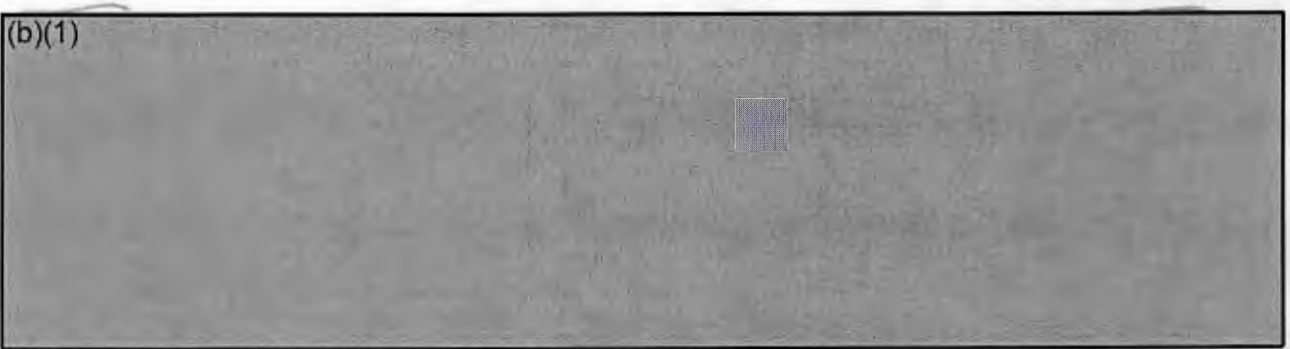
(b)(1)



c. (U) Select History of Terrorism:

- (1) (U) 1998: East Africa Embassy bombings: Kenya and Tanzania.
- (2) (U) 1999 and 2000: Thwarted millennium attacks: United States and Jordan.
- (3) (U) 2000: USS COLE attack: Yemen.
- (4) (U) 2001: World Trade Center and Pentagon attacks: United States

(b)(1)



~~SECRET~~
~~SECRET~~
~~SECRET~~

~~SECRET~~

~~SECRET~~

e. (U) Critical Capabilities

(b)(1)



(b)(1)

(2) (U) Leadership, inner circle, and senior advisers.

(3) (U) Planners and trainers.

(4) (U) Financial network.

(5) (U) Communications.

(b)(1)



2. (U) Egyptian Islamic Jihad (EIJ)

(b)(1)



c. (U) Select History of Terrorism

(b)(1)



~~SECRET~~

~~SECRET~~

(S)(U)

(b)(1)

e. (U) Critical Capabilities

- (1) (U) Leadership.
- (2) (U) Planners and trainers.
- (3) (U) Communications.
- (4) (U) Support infrastructure.

(b)(1)

3. (U) Gama'a al Islamiyya - Egyptian Islamic Group (IG)

(b)(1)

c. (U) Select History of Terrorism

(b)(1)

e. (U) Critical Capabilities

- (1) (U) External Leadership.
- (2) (U) Courier Network.

~~SECRET~~

~~SECRET~~

(U)

(3) (U) Communications.

(4) (U) Support infrastructure (safe houses).

(b)(1)

4. (U) Hizballah (Party of God) - Islamic Jihad Organization (IJO)

(b)(1)

c. (U) Select History of Terrorism

(b)(1)

e. (U) Critical Capabilities

(1) (U) Leadership.

(b)(1)

~~SECRET~~

~~SECRET~~

7 (b)(1)

(b)(1)

5. (U) Iranian Ministry of Intelligence and Security (MOIS)

a. (U) Profile. Iran's premier intelligence and security service and one of primary organs involved in supporting terrorism. The MOIS monitors expatriate Iranian communities, collects against antiregime groups, and conducts liaison with Islamic extremists worldwide.

(b)(1)

e. (U) Critical Capabilities

(b)(1)

~~SECRET~~

~~SECRET~~

(b)(1)

(b)(1)

5. (U) Iranian Ministry of Intelligence and Security (MOIS)

a. (U) Profile. Iran's premier intelligence and security service and one of primary organs involved in supporting terrorism. The MOIS monitors expatriate Iranian communities, collects against antiregime groups, and conducts liaison with Islamic extremists worldwide.

(b)(1)

e. (U) Critical Capabilities

(b)(1)

~~SECRET~~

~~SECRET~~

(b)(1)

(b)(1)

6. (U) Iranian Islamic Revolutionary Guard Corps - Qods Force (IRGC-QF)

(b)(1)

c. (U) Select History of Terrorism

(b)(1)

e. (U) Critical Capabilities

(b)(1)

~~SECRET~~

~~SECRET//NOFORN~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 3 TO ANNEX A TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

STATE SPONSORS (U)

(b)(1)



A-3-1

~~SECRET//NOFORN~~

(b)(1)

(b)(1)



a. (U) Continuing Support. Regimes that continue to provide material support to terrorist groups are the most active and dangerous of the states that sponsor terrorism. These countries are also highlighted on the DOS list of states sponsoring terrorism.

(b)(1)



(b)(1)

(b)(1)



b. (U) Residuals. Regimes that have distanced themselves markedly from their past sponsorship of terrorism are unlikely to support terrorist groups/acts in the future. Libya, the DPRK, and Cuba -- all currently found on the DOS list of states sponsoring terrorism -- are states that possess varying degrees of residual ties to terrorism.

(b)(1)



(b)(1)

~~SECRET//NOFORN~~

(L)(1)

(b)(1)



d. (U) Multiple Patterns. Some regimes will show parts or all of the connections to terrorism previously noted.

(b)(1)



~~SECRET//NOFORN~~

(b)(1)



~~SECRET//NOFORN~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 4 TO ANNEX A TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

(S)(1)

WEAPONS OF MASS DESTRUCTION (WMD) TERRORISM (U)

(b)(1)



~~SECRET//NOFORN~~
A-4-1
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1)

(b)(1)



2. (U) Technical Aspects of CBRN Terrorism

(b)(1)



~~SECRET//NOFORN~~

(b)(1)



~~SECRET//NOFORN~~

INTENTIONALLY BLANK

A-4-4

~~SECRET//NOFORN~~

~~SECRET~~

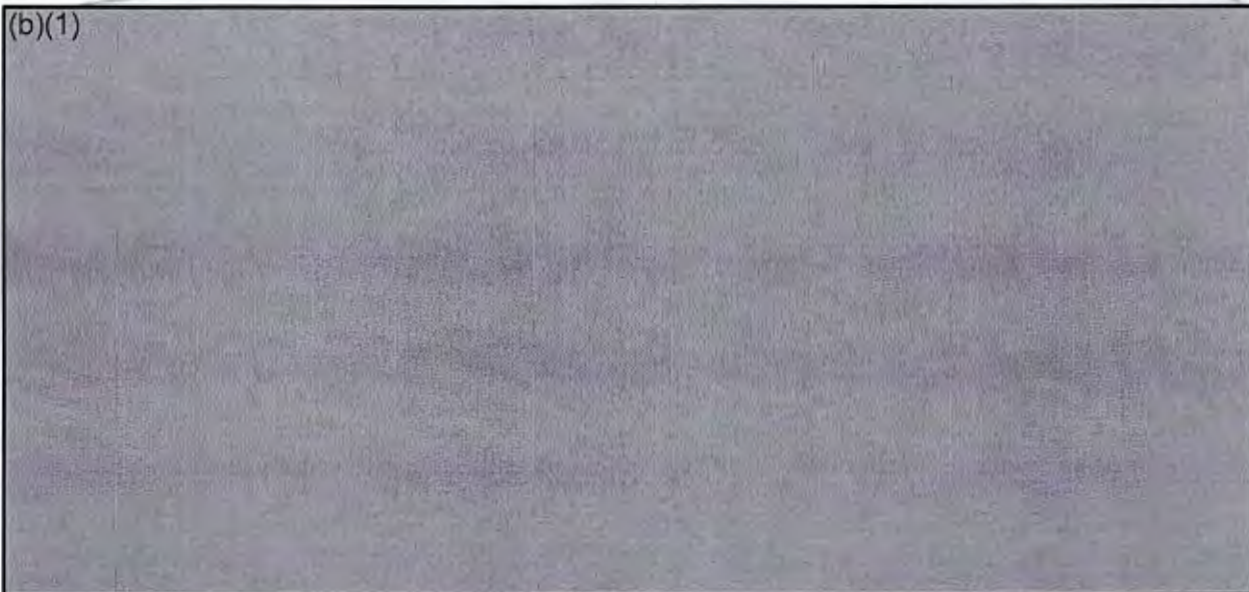
CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 5 TO ANNEX A TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

INTERROGATIONS (U)

(b)(1)

(b)(1)



2. (U) Joint Task Force Responsibilities

- a. (U) Procedures. Establish effective interrogation and information dissemination procedures among the interagency representatives supporting and/or participating in interrogations.

(b)(1)



(1)

~~SECRET~~

~~SECRET~~

(S)(1)

(b)(1)

f. (U) Interrogation standards. Establish worldwide standards of interrogation. Standards will largely reflect existing Service and joint doctrine on handling of detainees.

g. (U) Situational awareness. Maintain worldwide situational awareness of detainee operations and interrogations.

h. (U) Requirements. Define emerging requirements needed to support interrogation interview operations.

i. (U) Detainee disposition. Evaluate detainees to determine whether they pose a threat or are of intelligence value to the United States. Forward findings of such evaluations and recommendations for disposition to the Director, Joint Staff, via USSOUTHCOM, for forwarding to OUSD(P).

3. (U) Combatant Commander Responsibilities

(b)(1)

- (1) (U) Complete name, including all aliases.
- (2) (U) Identifying physical characteristics.
- (3) (U) Membership and rank or position in designated group.

~~SECRET~~

~~SECRET~~

- (4) (U) Fate of birth.
- (5) (U) City, county or province, and country of birth.
- (6) (U) Nationality and citizenship.
- (7) (U) Religion.
- (8) (U) Tribal affiliation, if any.
- (9) (U) Name and address of next of kin.
- (10) (U) Date and place of capture.
- (11) (U) Capturing unit.
- (12) (U) Circumstances of capture.
- (13) (U) General statement of health.

(b)(1)

(b)(1)

- (16) (U) Detainee's last known address.

(b)(1)

- (19) (U) Level of education (distinct from special skills).

(b)(1)

~~SECRET~~

(b)(1)

UNCLASSIFIED

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX B TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM

STRATEGIC MILITARY APPROACH

This annex provides written and graphic descriptions of the strategic concepts and anticipated military activities of the global war on terrorism. It also summarizes key strategic assumptions and planning principles.

1. Appendix 1 is a written and graphic description of the strategic approach as outlined in the main document. This strategic approach serves to synchronize planning efforts, and facilitate adaptation of the strategic approach over time. Appendix 1 will be a living document that is updated to incorporate changes in US policy decisions, interests, priorities, threats, and effects of previous operations.
2. Appendix 2 identifies the strategic assumptions of this plan.
3. Appendix 3 identifies the planning principles used to define the overall strategy for the war on terrorism.
4. Appendix 4 identifies the strategic framework to guide the planning process for the war on terrorism.

UNCLASSIFIED

INTENTIONALLY BLANK

B-2
UNCLASSIFIED

~~TOP SECRET~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 1 TO ANNEX B TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

STRATEGIC APPROACH TO THE WAR ON TERRORISM (U)

1. (U) This strategic approach serves to facilitate the iterative and adaptive planning of the war on terrorism over time. It will be continually updated with current guidance and assessments of risk, threat, and progress of US efforts.

a. (U) The strategic concept for the war on terrorism consists of a series of continuous, coordinated actions applying all of the elements of national power and conducted along multiple lines of operation to break the will of terrorist leaders, states, and nonstate actors that support terrorism, and deny terrorists access to WMD (see Figure 1, DOD Strategic Elements). The most immediate and serious threats will be addressed first. Operations will be targeted to expose vulnerabilities in terrorist networks and attack them. A territorial approach will be used to deny terrorist organizations safe haven and support from state sponsors and nonstate entities. Successes will be leveraged to dissuade and deter others from terrorist actions and support.

b. (U) Over time, the armed forces will leverage the successes of the Afghan campaign to maintain US strategic momentum in defeating terrorism while organizing for a sustained campaign.



Figure 1. Department of Defense Strategic Elements (U)

~~TOP SECRET~~
~~Reason: 1.6 (a)~~
~~Excluded from automatic downgrading and declassification~~

~~TOP SECRET~~

~~TOP SECRET~~

(b)(1)



7(4)(1)

Figure 2. Strategic Military Objectives (U)

(b)(1)



~~TOP SECRET~~

~~TOP SECRET~~

(b)(1)

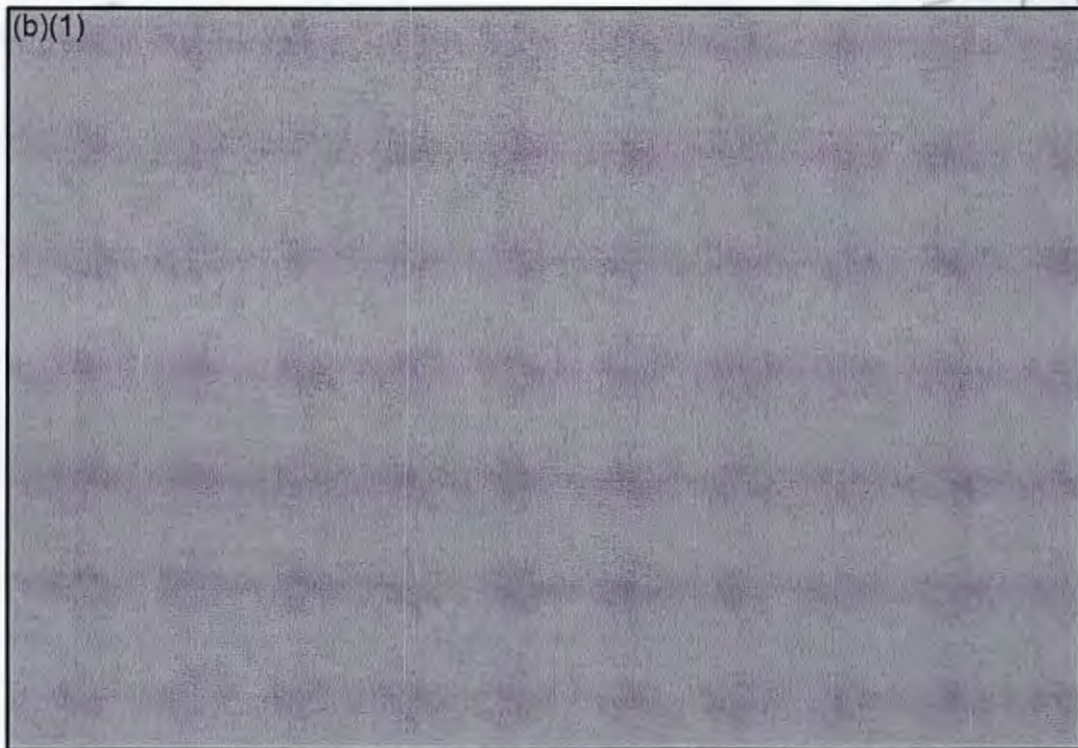
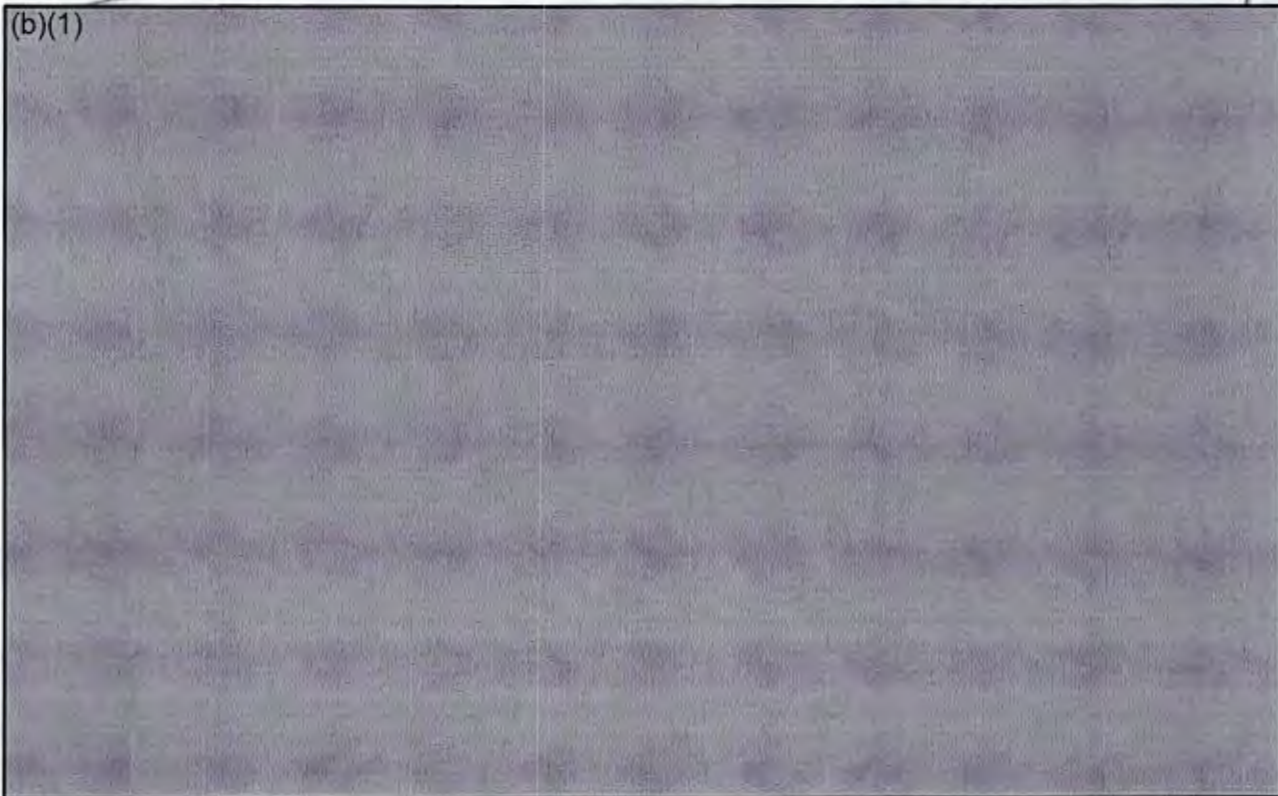


Figure 3. Military Objectives Over Time (U)



~~TOP SECRET~~

(b)(1)

UNCLASSIFIED

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 2 TO ANNEX B TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM

STRATEGIC ASSUMPTIONS

1. Terrorist organizations will retaliate against US and coalition interests worldwide.
2. Defeat of terrorist state sponsors will necessitate follow-on stability operations.
3. Support from other states will be constrained by conflicting domestic issues.
4. Existing Federal Response Plan (FRP) remains in effect.
5. US military will not be used to enforce US civil laws, unless otherwise directed by the President.
6. Initial reserve authorization remains valid for the near term; however, total reserve call-up may be required to support and sustain long-term operations.
7. Regional and global partners will require US assets and resources to support their deployment and employment.
8. Operations across combatant command areas of responsibility will be required.

B-2-1

UNCLASSIFIED

UNCLASSIFIED

INTENTIONALLY BLANK

B-2-2

UNCLASSIFIED

~~SECRET~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 3 TO ANNEX B TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

(b)(1)



B-3-1

~~SECRET~~

~~SECRET~~

INTENTIONALLY BLANK

B-3-2

~~SECRET~~

~~SECRET//NOFORN~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 4 TO ANNEX B TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM (U)

STRATEGIC FRAMEWORK (U)

(b)(1)



B-4-1

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
~~SECRET//NOFORN~~
~~SECRET//NOFORN~~
~~SECRET//NOFORN~~

~~SECRET~~

CHAIRMAN OF THE JOINT

CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX C TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM (U)

LEGAL CONSIDERATIONS (U)

1. (U) International Law

a. (U) Legal Basis for the Use of Force. A legal basis must exist for every decision to use military force in the global war on terrorism. Under customary international law, as reflected in the United Nations Charter, the United States has the inherent right of individual and collective self-defense against hostile acts or demonstrations of hostile intent toward the United States, its nationals, and assets. In addition, given the proper circumstances, the United Nations Security Council may authorize states to take action to restore international peace and security in a particular area. The UN Security Council has adopted several resolutions with respect to international terrorism. Though these resolutions do not confer any additional authority for the use of force, future such resolutions could do so.

b. (U) Rules of Engagement (ROE) and Rules for the Use of Force (RUF). Once the decision is made to use military force in the war on terrorism, ROE and RUF must exist for how that force will be applied. Careful attention must be paid to determining which ROE and/or RUF apply to the use of force during the missions assigned by the President, Secretary of Defense, and combatant commanders.

(b)(1)



(b)(6)



~~SECRET~~

~~SECRET~~

(2) ~~(S)~~ DOD Directive 5210.56 governs the carrying of firearms and rules for the use of force by DOD personnel performing law enforcement duties; also, in some areas of responsibility, RUF are supplemented by additional

(b)(1)

c. (U) Application of the Law of Armed Conflict. In accordance with DOD Directive 5100.77, it is the policy of the United States that US Armed Forces will comply with the law of armed conflict during all armed conflicts however such conflicts are characterized and, unless otherwise directed by competent authorities, will comply with the principles and spirit of the law of armed conflict during all other operations. The United States is a party to the 1949 Geneva Conventions.

2. (U) Domestic Law

(b)(1)

b. (U) Civil Support. US domestic law, Presidential directives, Executive Orders, and DOD directives provide the framework for and set limits on the use of military forces to assist civil authorities. While in a state active duty or title 32 status, the National Guard has primary responsibility for providing initial support to state and local authorities. When state and local government resources are exhausted or deemed inadequate, and when requested by appropriate authorities, the Department of Defense may provide federal military assistance under the direction of a designated lead federal agency. It is DOD policy that the Department of Defense will cooperate with and provide military assistance to civil authorities within the 50 states, District of Columbia, Commonwealth of Puerto Rico, US Virgin Islands, Guam, American Samoa, and Commonwealth of the Northern Mariana Islands, as directed by and consistent with applicable law, Presidential directives, Executive Orders, and DOD directives, including DOD Directive 3025.15. DODD 3025.15 is the umbrella directive that governs all DOD military assistance provided to civil

~~SECRET~~

~~SECRET~~

authorities, including military assistance for civil disturbances, military support to civil authorities, responses to acts or threats of terrorism, critical infrastructure protection, military support to civilian law enforcement agencies, and sensitive support.

c. (U) Posse Comitatus Act (PCA). Several laws and policies (most notably the PCA (18 USC 1385), 10 USC 375, and DOD Directive 5525.5) prohibit direct participation in civilian law enforcement activities that subject citizens to authority that is regulatory, proscriptive, or compulsory (e.g., interdiction of a vehicle, vessel, aircraft; search and seizure; arrest, apprehension, stop and frisk) by members of the Army, Navy, Air Force, or Marine Corps while on federal active duty. Use of military personnel for surveillance or pursuit of individuals or as undercover agents, informants, investigators, or interrogators is also prohibited. There are several exceptions and exclusions to these prohibitions. When undertaking military actions within the United States, commanders must ensure they are consistent with current law and policy on posse comitatus.

d. (U) Military Department Secretaries and Combatant Commanders' Title 10 Responsibilities. It is important to distinguish between the Military Department Secretaries' administration and support responsibilities under title 10 USC, sections 3013, 5013, and 8013 and the combatant commander's warfighting responsibilities under title 10 USC, sections 162 and 164. This distinction is the legal basis for assigning responsibilities, establishing or delegating command and support relationships, and establishing coordinating instructions between joint forces and their components. Subject to the authority, direction, and control of the Secretary of Defense and the command authority of the combatant commanders (as prescribed in title 10 USC, section 164), the secretaries are responsible for, and have the authority necessary to conduct all affairs of their respective Departments. The secretaries fulfill their title 10 responsibilities by exercising administrative control (ADCON) through the Service component commanders assigned to the combatant commands. ADCON is synonymous with the secretaries' administration and support responsibilities under title 10.

~~SECRET~~

~~SECRET~~

INTENTIONALLY BLANK

C-4

~~SECRET~~

~~SECRET~~

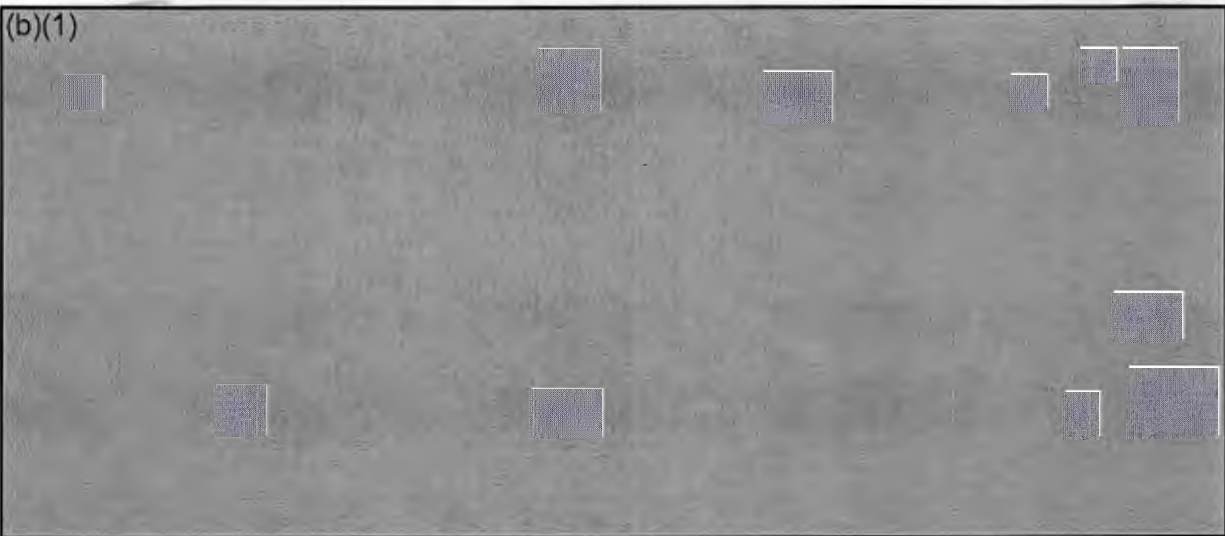
CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX D TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM (U)

INFORMATION OPERATIONS (U)

1. (U) DOD Information Operations (IO) Objectives

(b)(1)

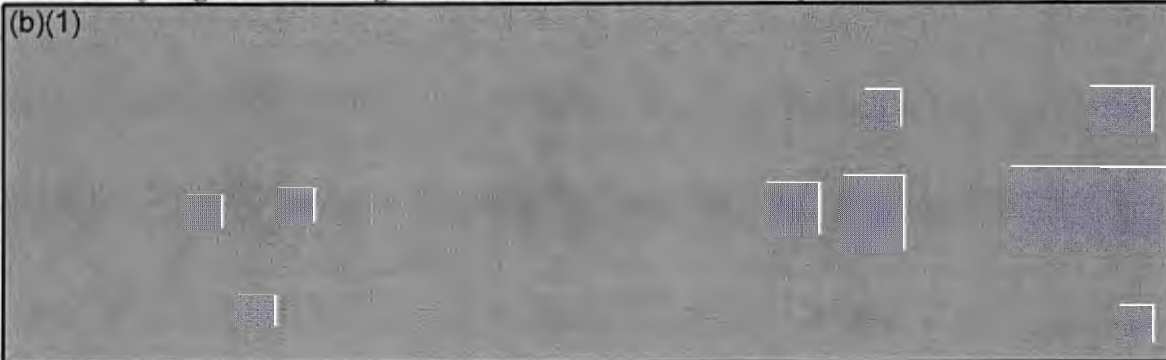


2. (U) Situation

a. (U) Global Information Environment

(1) ~~(S)~~ The 11 September 2001 terrorist attacks on the United States created a markedly higher level of global concern and uncertainty that is increasingly

(b)(1)



~~SECRET~~

~~SECRET~~

(2)(U)

(b)(1)



b. (U) Friendly Situation. See base plan.

(b)(1)



3. (U) Execution

(b)(1)

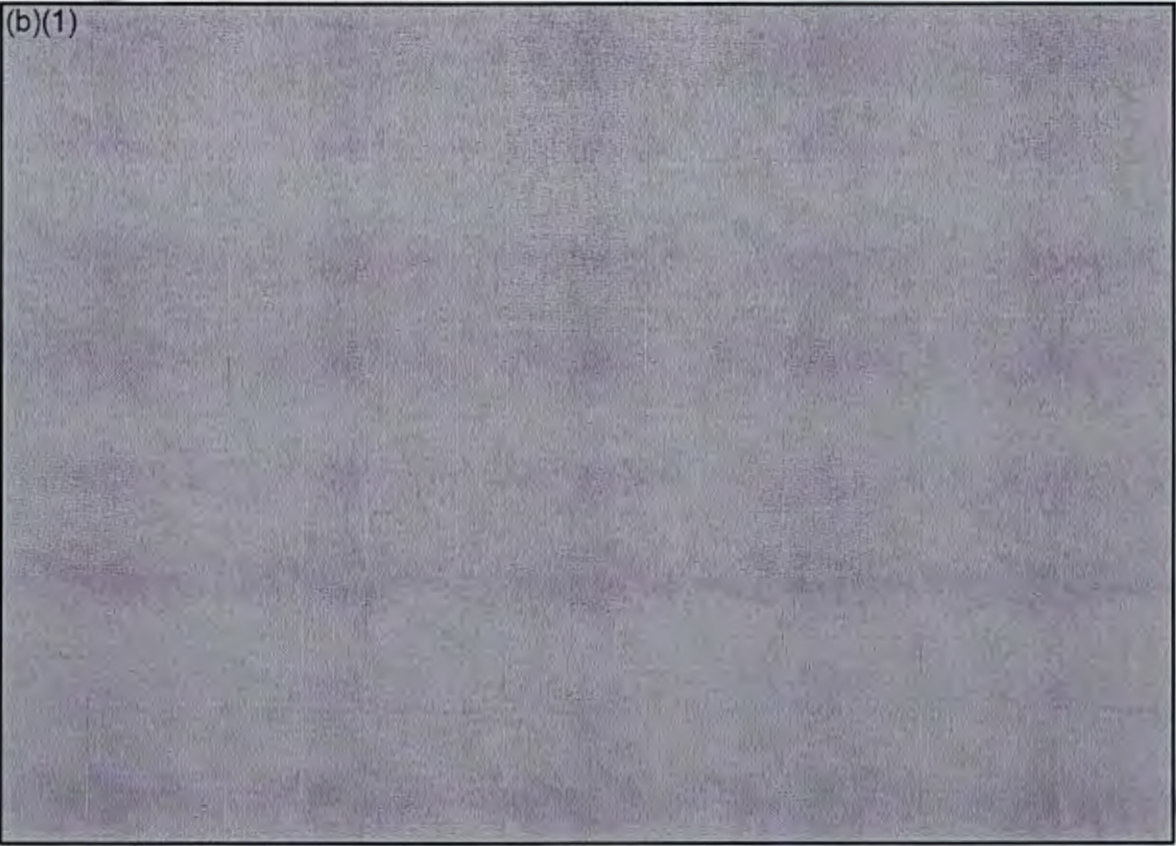


~~SECRET~~

~~SECRET~~

(b)(1)

(b)(1)



c. (U) Functions

(1) (U) Deputy Directorate for Information Operations, DDIO (J39).

(a) (U) Synchronizes, deconflicts and coordinates combatant commanders' IO plans.

(b) (U) Integrates IO functions across the Department of Defense and serves as a point of entry for the combatant commanders to the interagency process.

(c) (U) Observes and analyzes the strategic information environment, and provides recommended courses of action to DOD and appropriate government agencies.

(2) (U) USSTRATCOM. Assist the Joint Staff, through the DDIO, in development, coordination, deconfliction and synchronization of combatant commander's IO plans.

(3) (U) Combatant Commands. As outlined in the base plan.

~~SECRET~~

~~SECRET~~

4. (U) Administration and Logistics. See base plan.
5. (U) Command and Control. See base plan.

~~SECRET~~

~~SECRET~~

INTENTIONALLY BLANK

D-6

~~SECRET~~

UNCLASSIFIED

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX E TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM

COALITION MANAGEMENT

1. Situation

a. The global war on terrorism will be fought with all elements of national power: diplomatic, informational, economic, and military. It will also require an unprecedented level of coordination among law enforcement authorities. To achieve its national strategic objectives, the United States must synchronize the application of these elements of power-- preferably in coordination with other nations. To that end, depending on military requirements derived from specific missions given to US forces by the President or Secretary of Defense, it is important that the United States have the capability to form multinational coalitions that can adapt, change, and evolve throughout the execution of the conflict.

b. Although the United States should be prepared to act unilaterally if necessary, coalitions can contribute significantly to mission accomplishment. Military contributions from these coalitions provide assets that enhance the ability of coalition forces to simultaneously strike against terrorism in multiple regions, and can allow sustained focus of military power on a main effort while supporting operations contributing globally. Politically, mission-specific coalitions lend legitimacy to the Nation's efforts by demonstrating a unified resolve to fight terrorism.

c. Additionally, through the careful use of coalition forces, the United States can mitigate risk of over commitment elsewhere to regional hot spots (e.g., the Korean Peninsula, Iraq, and China-Taiwan). Use of coalition forces may assist in reducing the impact of military operations on Operational Tempo (OPTEMPO), Personnel Tempo (PERSTEMPO), Global Military and Naval Force Power Projection (GNFPP/GMFPP), and help offset the impact of budget expenditure reductions on force levels.

2. Managing Coalition Contributions

a. Having the capability to build and maintain coalitions is an essential part of the NMSP-WOT. Every offer of support is politically important, no

UNCLASSIFIED

matter how militarily significant. It is important for combatant commands to recognize the political value of force offers, while balancing their military requirements. Although there is no requirement for combatant commands to accept offers of coalition support, careful consideration of both coalition force offers and regional restrictions on overflight, access, and basing are necessary.

b. The types of support offered by coalition participants are displayed graphically in Figure E-1. Relative military importance is displayed by support area. From the purely military perspective the top three or four are most significant and have been the focus of the Joint Staff efforts. The absence of identified offers of coalition support should not constrain combatant command requirements.



Figure E-1. Notional Hierarchy of Coalition Support (U)

c. As combatant commands develop their detailed operational plans, they are strongly encouraged to identify requirements, particularly potential basing, access, and overflight requirements, to the Chairman of the Joint Chiefs of Staff as early in the planning process as practical. Experience shows that the diplomatic coordination for partnership country access to other host nations can be problematic and often requires additional time for negotiation.

d. In addition to support to be received from coalitions, combatant commanders must consider and estimate the support required by these coalitions from the United States. The costs of accepting offers of support must

UNCLASSIFIED

be weighed against the anticipated military and/or political benefits to be gained.

3. Coalition Approval Process. The responsibility for building this coalition rests jointly with both the Departments of Defense and State. The Interagency (IA) approval process for specific offers of support requires the approval of both the Secretary of Defense and Secretary of State. The process is structured in two phases. The first phase, "Political Approval," decides whether a country will be admitted into the coalition and accepts or declines a country's offer of support. The second phase, "Force Approval," reviews combatant command requests of coalition forces and approves or disapproves the combatant commander's request for forces. This process is displayed in Figure E-2:

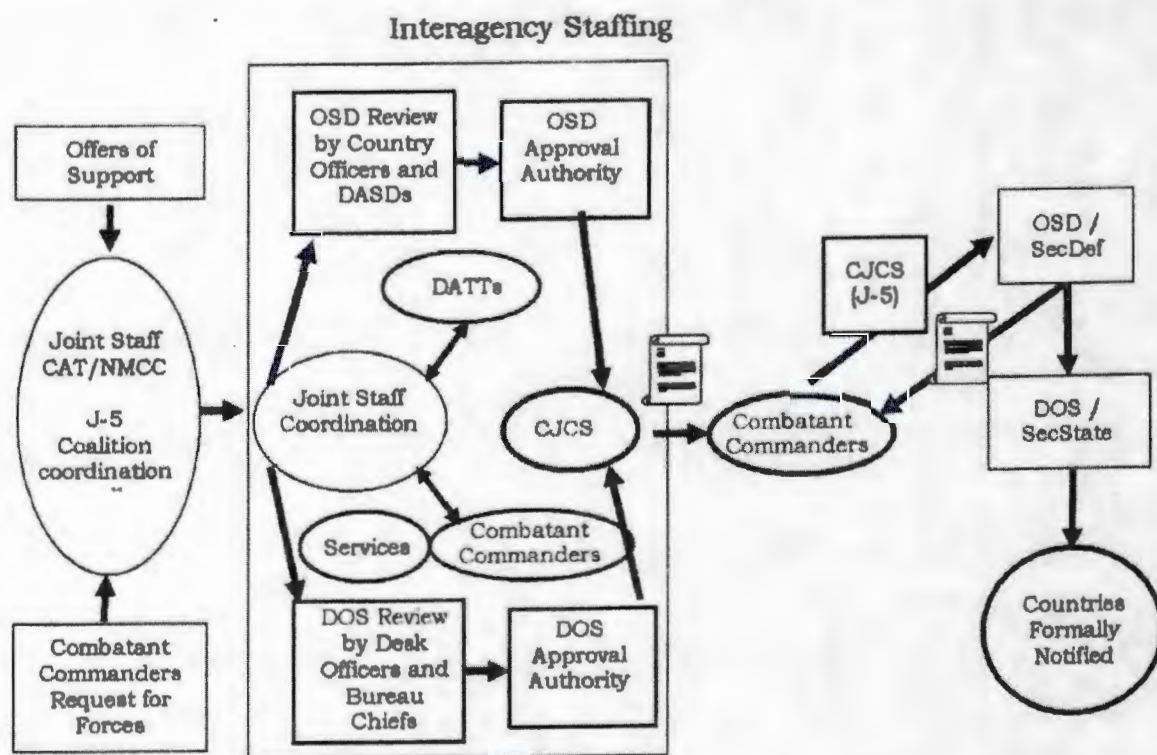


Figure E-2 - Approval Process

b. Political Approval

(1) Foreign government offers of support are received through White House, DOS, DOD, or other channels. The receiving agency informs DOS of the offer and DOS will validate and acknowledge the offer through diplomatic

UNCLASSIFIED

channels. Once validated, the Joint Staff is notified and the offer is entered and tracked on the Joint Staff Enduring Freedom Coalition Support Matrix.

(2) DOS, OSD, and the Joint Staff review the offer from both foreign policy and military utility basis based on current and potential future military operations. Offers are considered for a broad range of missions in addition to direct action, to include operational support, peacekeeping operation offsets, and support for humanitarian assistance operations. All offers are further staffed with the combatant commands, Services, and Defense Attaches for comment prior to forwarding to the Chairman of the Joint Chiefs of Staff for decision. The Chairman recommends approval or disapproval of military use of foreign force offers to the Secretary of Defense.

(3) Once the political decision is made to accept the offer of foreign military support, a Joint Staff message is transmitted to all combatant commands granting permission to initiate informal military-to-military contact with the country to determine specific military capabilities of the support offered. This message further authorizes combatant commanders to accept liaison officers from those nations, but precludes combatant commanders from accepting military force offers at this phase of the process.

c. Force Approval

(1) Following the determination of coalition force requirements, combatant commanders forward a Request for Forces (RFF) message through the Chairman of the Joint Chiefs of Staff (J3/vice director or agency) to the Secretary of Defense requesting foreign military capability in support of both current and potential future operations.

(2) The Joint Staff coordination process for force approval mirrors the political approval procedure above.

(3) Once approved by the Director, Joint Staff, and the appropriate Assistant Secretary of Defense, a Joint Staff message is sent to combatant commands authorizing the forces requested and directing coordination with the contributing country. At this time, commands begin to coordinate mission, deployment, sustainment, and command and control relationship issues with the offering partner. Additionally, DOS informs the foreign government of acceptance of specific forces through diplomatic channels. If the country's support is not presently required, DOS informs the foreign government and the option for future acceptance of the offer for other missions is left open.

(4) Combatant commands must identify the preferred beddown requirements at the time that the RFF is submitted. DOS will solicit initial

UNCLASSIFIED

diplomatic authorization for base access and overflight from the governments of deployment locations concurrent with the RFF approval process.

(5) Advance Agreements such as SOFAs and ACSAs should serve as precursor to any "next steps" consideration. The United States must secure freedom of movement within all AORs to ensure success. It is prudent in conducting the WOT to have as many agreements in place as possible to ensure leverage, influence and presence as well as the required flexibility. Early diplomatic negotiations will secure these agreements while not being constrained by pressure and time requirements. It is less prudent to attempt when there are conditions of immediacy. The conditions for securing agreements in advance should present an environment that is much more conducive to achieving the desired end state.

(6) Combatant command concerns and questions regarding the development of agile partnerships should be directed to the Joint Staff, J-5, Coalition Coordination Cell for resolution.

UNCLASSIFIED

INTENTIONALLY BLANK

E-6

UNCLASSIFIED

~~CONFIDENTIAL~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX F TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM (U)

THEATER SECURITY COOPERATION (U)

- (U) References:
- a. Defense Planning Guidance, August 2001
 - b. Quadrennial Defense Review, 30 September 2001
 - c. CJCSI 3110.01D, Joint Strategic Capabilities Plan, 20 July 2001
1. (U) General. This annex provides guidance for the planning and execution of supporting theater security cooperation (TSC) programs and activities.
2. (U) Situation
- a. (U) Concept for TSC
- (1) (U) TSC is an integrated series of activities that, among other goals and aims, help set the initial conditions for future military action in terms of combined capabilities, US access, interoperability, and intelligence sharing.
- (2) (U) TSC activities, planned and executed in peacetime, include the development of improved access for US forces and are intended to support combatant commanders OPLANs, CONPLANs, functional plans, and the evolving global war on terrorism.
- (3) (U) TSC programs support allied transformation efforts and are intended to improve the capability of key countries to assume a larger role in regional and global security matters.
- (4) (U) Existing TSC programs and supporting activities offer a wide range of support to the war on terrorism. Examples include the following:
- (a) (U) Military-to-military contacts.
 - (b) (U) Intelligence sharing.

~~CONFIDENTIAL~~
~~CONFIDENTIAL~~
~~CONFIDENTIAL~~
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- (c) (U) Equip-and-train activities with foreign forces.
- (d) (U) Security assistance team visits.
- (e) (U) Security assistance programs (FMS, FMF, grants, and IMET).
- (f) (U) Humanitarian assistance, peacekeeping, and stability operations.
- (g) (U) Counterterrorism, counterdrug, counterproliferation, and CM training, exercises, and education.
- (h) (U) JCET.
- (i) (U) Reciprocal and/or reimbursable training (including acquisition and cross-servicing agreements).
- (j) (U) Foreign internal security and/or defense training and assistance.
- (k) (U) Treaty and arms control agreements (NPT, CWC, CTR).
- (l) (U) Counterdrug support and counterdrug operations.

(b)(1)



D. (U) Assumptions

- (1) (U) Sufficient resources are available to execute combatant commanders TSC plans.
- (2) (U) Planned TSC activities will be executed.

C. (U) Planning Factors

(b)(1)



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(b)(1)



(b)(1)

d. (U) Resource Availability. Force apportionment will be in accordance with reference c. Regional combatant commanders will identify critical TSC resource shortfalls within their TSC strategies.

(b)(1)



a. (U) Functional Combatant Commanders (USSOCOM, USJFCOM, USSTRATCOM, USTRANSCOM). Forward supporting plan inputs to the combatant commanders during the TSC plan development phase within 30 days of the issuance of TSC guidance.

(b)(1)



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

INTENTIONALLY BLANK

F-4

~~CONFIDENTIAL~~

~~SECRET~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX G TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM (U)

HOMELAND SECURITY (U)

- (U) References:
- a. United States Government Interagency Domestic Terrorism Concept of Operations Plan, 31 January 2001; Internet address:
<http://www.fbi.gov/publications/conplan/conplan.pdf>.
 - b. DODD 2000.12, 13 April 1999, "Antiterrorism/Force Protection (AT/FP) Program"; Internet address:
<http://www.dtic.mil/whs/directives/corres/dir1.html>.
 - c. CONPLAN MC 100-34, 9 August 2001, "CANADA-UNITED STATES Combined Defense Plan (CDP)"
 - d. NORAD CONPLAN 3310-96, Change 2, "Air Sovereignty and Aerospace Defense of North America," 24 September 1999
 - e. Federal Emergency Management Agency, 9230-1-PL, "Federal Response Plan (FRP), with Terrorism Incident Annex," April 1999; Internet address:
<http://www.fema.gov/r-n-r/frp/frpterr.htm>.
 - f. Federal Emergency Management Agency, 1 May 1996, "Federal Radiological Emergency Response Plan"
 - g. PRESIDENTIAL DECISION DIRECTIVE/NSC 63, 22 May 1998, "Critical Infrastructure Protection"; Internet address:
<http://fas.org/irp/offdoc/pdd/index.html>.
 - h. DODD 5160.54, 11 August 1999, "Critical Infrastructure Protection"; Internet address:
<http://www.dtic.mil/whs/directives/corres/dir2.html>.
 - i. DOD Instruction 2000.16, 14 June 2001, "Antiterrorism Standards"; Internet address:
<http://www.dtic.mil/whs/directives/corres/dir1.html>.
 - j. CJCSI 3110.16, 10 November 2000, "Military Capabilities, Assets, and Units for Chemical, Biological, Radiological, Nuclear and High Yield Explosive Consequence Management Operations"

~~SECRET~~
~~SECRET~~
~~SECRET~~
~~SECRET~~

~~SECRET~~

~~SECRET~~

- k. DOD Instruction 5030.34, 17 September 1986, "Agreement Between the US Secret Service (USSS) and the DOD Concerning Protection of the President and Other Officials"; Internet address:
<http://www.dtic.mil/whs/directives/corres/ins1.html>.
- l. Executive Secretary, OSD memorandum, 20 June 1990, "DOD Explosive Ordnance Disposal (EOD) Support to the USSS and the Department of State (DOS)"
- m. Operations Plan for EOD Very Important Persons Protection Support Activity (VIPPSA) to the USSS and DOS, 17 February 2000
- n. CJCS CONPLAN 0300 (S/FP) and US Combatant Commanders JFCOM CONPLAN 0500 (DRAFT)
- o. CJCSI 3125.01, 3 August 2001, "Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Nuclear, Radiological and High Yield Explosive Situation"
- p. Presidential Executive Order Establishing Office of Homeland Security, 8 October 2001
- q. Unified Command Plan, 29 September 1999, with Secretary of Defense cover memorandum to the President of the United States, 13 September 1999
- r. Secretary of Defense Memorandum, 1 April 2000, "Consequence Management Responsibilities within DOD Incidents Involving Chemical, Biological, Radiological, Nuclear, and High Yield Explosives"
- s. Secretary of Defense Memorandum, 10 August 2000, "Management of DOD Operational Response to the Consequence of Certain Incidents Involving Chemical, Biological, Radiological, Nuclear and High Yield Explosives"
- t. Appendix 16 (6 September 2001), Annex C, JOPES Volume II
- u. PRESIDENTIAL DECISION DIRECTIVE/NSC 62, "Protection Against Unconventional Threats to the Homeland and Americans Abroad", 22 May 1998
- v. Execution Order, CJCS 161950Z Oct 01
- w. DODD 3025.12, 4 February 1994, "Military Assistance for Civil Disturbances (MACDIS)"
- x. DODD 3025.15, 18 February 1997, "Military Assistance to Civil Authorities (MACA)"
- y. DODD 3025.1, 15 January 1993, "Military Support to Civil Authorities (MSCA)"
- z. DODD 5210.56, November 2001, "Use of Deadly Force and Carrying of Firearms by DOD Personnel Engaged in Law

~~SECRET~~

~~SECRET~~

Enforcement and Security Duties"

aa. CJCS CONPLAN 0500-98 DRAFT, "Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Nuclear, Radiological, or High-Yield Explosive Situation"

1. (U) Situation

a. (U) General. Home Land Security (HLS) is a national responsibility and consists of Homeland Defense (HLD) and Civil Support (CS) mission areas. Ensuring the security of the homeland requires coordination and cooperation among the Department of Defense, the Interagency (IA), and state and local authorities.

(1) (U) This annex outlines enduring strategic military requirements and responsibilities for enhancing and institutionalizing the security of the US homeland. It does not override requirements established either by current law or existing policy; rather, the purpose is to provide strategic guidance for HLS operations in support of the NMSP and the global war on terrorism. Military assistance to civil authorities (MACA) will be conducted in accordance with established policies, plans, or directives unless otherwise directed. (S)(1)

(b)(1)



~~SECRET~~

~~SECRET~~

c. (U) Deterrent Options

(1) (U) The Director, Office of Homeland Security, in coordination with the interagency, continues to evaluate known and emerging threats to the homeland, to develop a national threat warning system and to issue threat advisories or alerts as appropriate. These alerts and advisories will provide a standardized national threat process that articulates the level of terrorist threat to the Nation and provides federal, state, and local agencies a means to escalate their levels of preparedness. This national advisory system will complement, but not replace, DOD current force protection levels.

(2) (U) Service Chiefs implement force protection condition measures in order to establish a deterrent and harden DOD installations against possible terrorist attack. Random force protection exercises will improve installation-level preparedness, the security of DOD facilities, and protection of DOD critical infrastructure. (b)(1)

(b)(1)



(7) (U) Selective mobilization of the Reserve Component Forces (RCF) will provide additional forces available for this critical mission and will also serve to heighten awareness in the civilian community and be a continuing reminder of the need for vigilance.

~~SECRET~~

~~SECRET~~

(b)(1)

d. (U) Enemy Forces

(b)(1)



(2) (U) Enemy Courses of Action (COA)

(a) (U) Most Likely COA

(b)(1)



(b) (U) Most Dangerous COA

(b)(1)



(3) (U) Current Threat Situation. See J-2 Intelligence Executive Summary at Annex A.

~~SECRET~~

~~SECRET~~

e. (U) Friendly Forces and Agencies

(1) (U) Office of Homeland Security (OHLS). OHLS is the designated executive office charged by the President to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist attacks or threats. OHLS will coordinate federal efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

(2) (U) Department of Homeland Security (DHLS). If approved by Congress, DHLS will serve as the unifying core of the vast national network of organizations and institutions involved in homeland security. DHLS will bring together 22 entities with critical homeland security missions within a single federal department whose primary mission is to protect our homeland against terrorist threats. While being focused primarily on homeland security, the department will continue to execute the nonhomeland security missions of its constituent parts.

(3) (U) Department of Justice. The Attorney General is responsible for ensuring the development and implementation of policies directed at preventing terrorist attacks domestically. DOJ has charged the Federal Bureau of Investigation with execution of its lead federal agency (LFA) responsibilities for the management of a federal response to terrorist threats or incidents that take place within US territory, or those occurring in international waters that do not involve the flag vessel of a foreign country. In that role, a representative of the Attorney General will normally operate as the on-scene commander for the Federal Government.

(4) (U) Federal Emergency Management Agency (FEMA). FEMA is the primary federal coordinating agency for disaster response and recovery activities, whether manmade or natural. FEMA uses the existing FRP structure to manage and coordinate the federal response to consequences of terrorism, including the consequences of CBRNE. FEMA is responsible for conducting consequence management (CM) contingency planning, and will be the lead agency for CM. (S U)

(b)(1)



~~SECRET~~

(b)(1)

f. (U) Facts

(b)(1)

(4) (U) The US Coast Guard will continue to serve as the lead agency for maritime security unless the President directs the Secretary of Defense to undertake this mission.

(5) (U) Pending establishment and consolidation of HLS-related functions into a specific office within the Office of the Secretary of Defense, the Secretary of the Army will remain the Executive Agent for military assistance to civil authorities and the Director of Military Support will remain the action agent for tasking of military support to civil authorities for requests approved by the DOD Executive Secretary.

(6) (U) In accordance with the Federal Response Plan (FRP), including the terrorism annex and the Federal Radiological Emergency Response Plan, the Department of Defense will provide military assistance to civil authorities, as directed by the President or Secretary of Defense.

(7) (U) Coordination with Canadian and Mexican authorities will be conducted through DOS and Joint Staff until implementation of UCP 2002 on 1 October 2002. Responsibilities will then pass to USNORTHCOM. Canada and US command relationships will be in accordance with Canada-US Basic Security Document, MCC 100-35; the NORAD agreement, NORAD CONPLAN 3310; and the Combined Defense Plan.

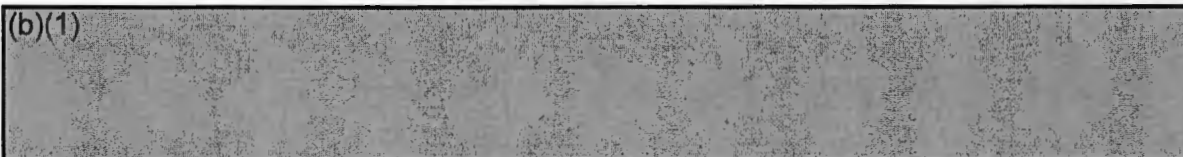
(8) (U) Definitions. Current interim definitions and construct, coordinated with combatant commanders and Services are as follows:

(a) (U) Homeland Security. In accordance with National Strategy for Homeland Security, "Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. Also called HLS. See also Homeland Defense and Civil Support.

(b) (U) Homeland Defense. The protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called HLD. See also Homeland Security and Civil Support.

(c) (U) Civil Support. DOD support to US civil authorities for domestic emergencies and for designated law enforcement and other activities. Also called CS. See also Homeland Security and Homeland Defense.

g. (U) Limitations and Constraints

(b)(1) 

(2) (U) AC and RC units are multiapportioned for other JSCP requirements.

(3) (U) There are shortages of interoperable civil communications systems in military units and military communications systems in civilian organizations.

(4) (U) The Joint Staff will coordinate HLS issues for all combatant commanders with the OHLS; direct coordination with OHLS by other than the Joint Staff is not authorized.

h. (U) Legal Considerations. See Annex C.

~~SECRET~~

(b)(1)

i. (U) Risks

(b)(1)



(3) (U) Critical Infrastructure Protection (CIP)

(b)(1)



~~SECRET~~

(b)(1)



~~SECRET~~

(b)(1)

(b)(1)



3. (U) Execution

a. (U) Intent

(b)(1)



(2) (U) Method

(b)(1)



~~SECRET~~

~~SECRET~~

(b)(1)



(b)(1)

c. (U) Tasks.

(1) (U) Joint Staff

(b)(1)



~~SECRET~~

~~SECRET~~

(6)(1)

(b)(1)

A rectangular area of the document is completely redacted with a solid black fill.

(2) (U) Commander, USNORTHCOM

(b)(1)

A large rectangular area of the document is completely redacted with a solid black fill, covering the majority of the page's content.

(3) (U) Commander, USPACOM.

(b)(1)

A rectangular area of the document is completely redacted with a solid black fill.

~~SECRET~~

~~SECRET~~

(b)(1)

(b)(1)



(4) (U) Commander, USSOUTHCOM

(b)(1)



G-15

~~SECRET~~

~~SECRET~~

(b)(1)

(b)(1)

(5) (U) CDRUSELEMNORAD

(b)(1)

(6) (U) Commander, USTRANSCOM. As directed, provide deployment, employment, and redeployment common-user air, land, and sea transportation for forces engaged in HLS operations and provide aeromedical evacuation as required.

(b)(1)

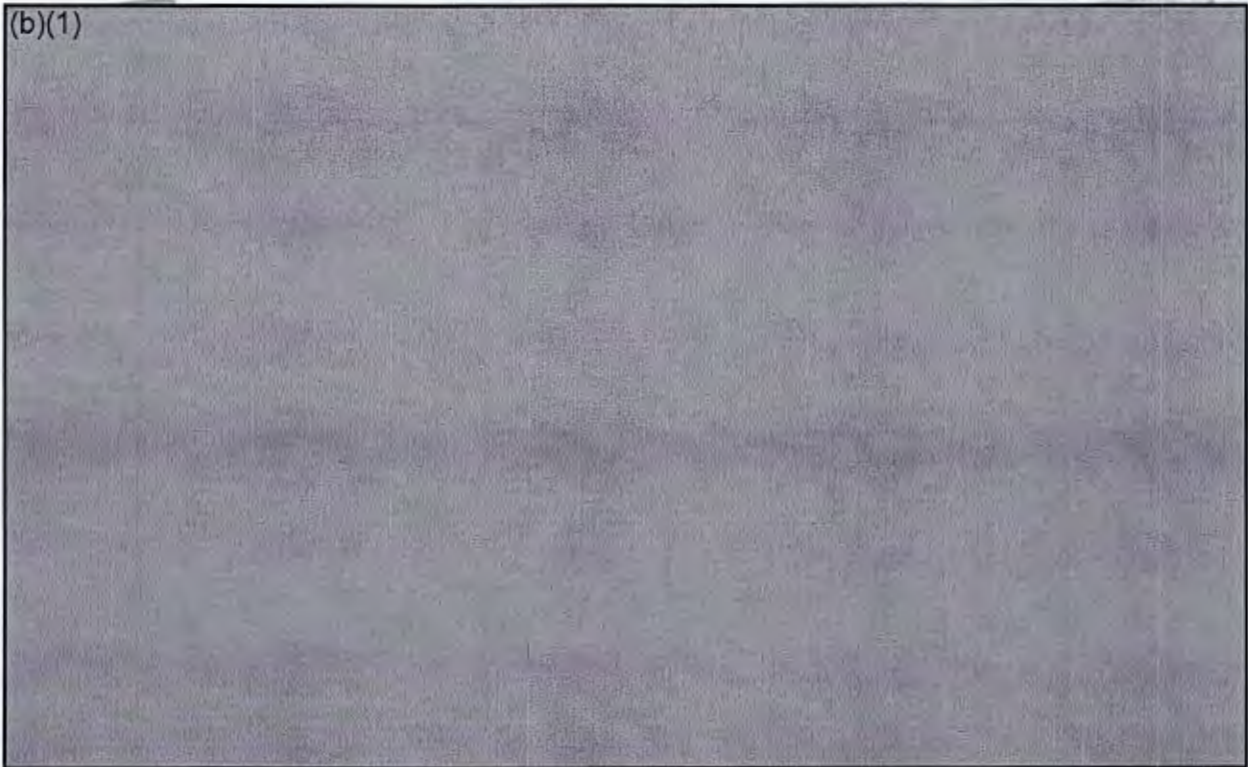
(8) (U) Commander, USSTRATCOM.

(b)(1)

~~SECRET~~

(b)(1)

(9) (U) Military Services



(10) (U) USCG (Lead Federal Agency for the Maritime Domain)

(a) (U) As directed by appropriate authority, USCG is expected to: provide for harbor security and defense in coordination with USNORTHCOM, USPACOM, USSOUTHCOM, and US Navy.

(b) (U) Monitor marine shipments of hazardous materials and be prepared to respond in accordance with the FRP and National CONPLAN.

(c) (U) When directed, conduct sustainable port security operations by employing interoperable joint, multiagency forces including cooperation with private industry security forces.

(d) (U) When directed, provide force protection during military upload and download of forces and equipment in direct support of military operations. Coordinate and support safety and security efforts for other military uploads or download of forces and equipment in support of USTRANSCOM.

~~SECRET~~

(e) (U) As directed, protect critical infrastructure based on a tier priority list and a continuum of protection tailored to changes in Maritime Security (MARSEC) level. Three levels of security posture for ports, waterways, maritime facilities, and adjacent waters are being established. MARSEC level 1 is the desired state. MARSECs 2 and 3 are surge levels that bring additional assets to commanders for use in developing specific tailored responses to identified threats. Develop streamlined procedures to request appropriate DOD support for all MARSEC levels.

(f) (U) Maintain maritime commercial throughput at US ports, with priority given to strategic seaports.

(g) (U) Coordinate and conduct coastal surveillance of the United States and territories, including off-shore structures. Detect the maritime threats to the United States.

(h) (U) Coordinate and conduct Maritime Interception Operations of threatening marine targets and high-interest vessels before they enter US ports.

(i) (U) Synchronize intelligence efforts to enhance port security operations and coastal patrol efforts. Promote Maritime Domain Awareness.

(j) (U) Coordinate mine countermeasure operations and counters to other underwater threats with DOD, state/local agencies, and commercial diving enterprise.

(k) (U) Conduct port vulnerability assessments to identify port and critical infrastructure vulnerabilities and provide recommendations for improvement.

(l) (U) Form Port Security Committees or Security Subcommittees of existing Harbor Safety Committees in each major port.

(m) (U) Review, approve, and exercise required public/private port, vessel, and facility security plans.

(n) (U) Develop public/private outreach to expand partnerships. Employ appropriate voluntary organizations, including Coast Guard Auxiliary, Civil Air Patrol, Power Squadrons, and others, in all Coast Guard missions consistent with threats and capabilities.

(o) (U) Identify to combatant commanders those DOD forces that are required to conduct maritime HLS.

~~SECRET~~

~~SECRET~~

(b)(1)

d. (U) Coordinating Instructions

(b)(1)

(2) (U) Comply with Restricted Operations Zones to support protection of critical sites from air attack and preclude engagement from friendly fire.

(3) (U) All coordination with OHLS will be conducted through the Joint Staff.

e. (U) Use of Weapons and Rules on the Use of Force. Use of weapons policies and RUF/ROE applicable to DOD personnel vary according to the assigned mission and specific AOR. Neither the ROE nor RUF limit a commander's inherent authority and obligation to use all necessary means available and to take all appropriate action in self-defense of the commander's unit and other US forces in the vicinity. Specific changes to ROE and appropriate RUF will be requested by the combatant commander, approved by the Secretary of Defense, and promulgated by the Chairman of the Joint Chiefs of Staff.

4. (U) Logistics. Primary logistical focus for all phases will be on efforts to protect, support, and sustain forces employed in HLS. The protection of depots, supply centers, transportation hubs, and other designated critical infrastructure that supports deployment is also essential in all phases. Secondary logistical effort will be military support to civil authorities unless otherwise directed.

5. (U) Command and Control

a. (U) The Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, will determine the appropriate command relationships (supported and supporting commanders) for each specific contingency.

b. (U) Specific HLS command relationships are as specified in base order.

~~SECRET~~

~~SECRET~~

INTENTIONALLY BLANK

G-20

~~SECRET~~

~~TOP SECRET~~

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

ANNEX H TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR ON
TERRORISM U)

IMPLEMENTATION (U)

1. (U) Purpose. To provide guidance and a general framework for implementing and updating the National Military Strategic Plan for the War on Terrorism (NMSP-WOT).
2. (U) General. The NMSP-WOT is a living document that facilitates iterative and adaptive planning over time to maintain strategic focus and momentum in the war effort. It facilitates planning to set the conditions for decisive operations and identifies opportunities. The risks and opportunities presented during the war on terrorism will be identified and analyzed by the Strategic Planning Team (SPT). The SPT will review and continually validate the effectiveness of the NMSP-WOT and develop recommendations to the Executive Steering Group (ESG) to shape the direction of the war on terrorism. The ESG will provide military advice and recommended strategic direction to the Joint Chiefs of Staff and the Secretary of Defense.
3. (U) Implementation Process. As directed in the Contingency Planning Guidance (2002), the Chairman of the Joint Chiefs of Staff will develop and implement a strategic planning process to achieve the military strategic objectives for the global war on terrorism. This process will include strategic plans and functional reviews that facilitate prioritizing, coordinating, and assessing actions, on both a regional and global scale.
 - a. (U) Routine and continuous updates of the strategy will ensure consistency with US policy and the intent of the Secretary of Defense and the President. Risk assessments and mitigation efforts are an essential component of this process. Assessing the risks associated with the ability of the US military to concurrently execute this war and other military requirements in the Defense Strategy will be crucial when advising the President and Secretary of Defense on force employment options.

~~TOP SECRET~~
~~TOP SECRET~~
~~TOP SECRET~~
~~TOP SECRET~~

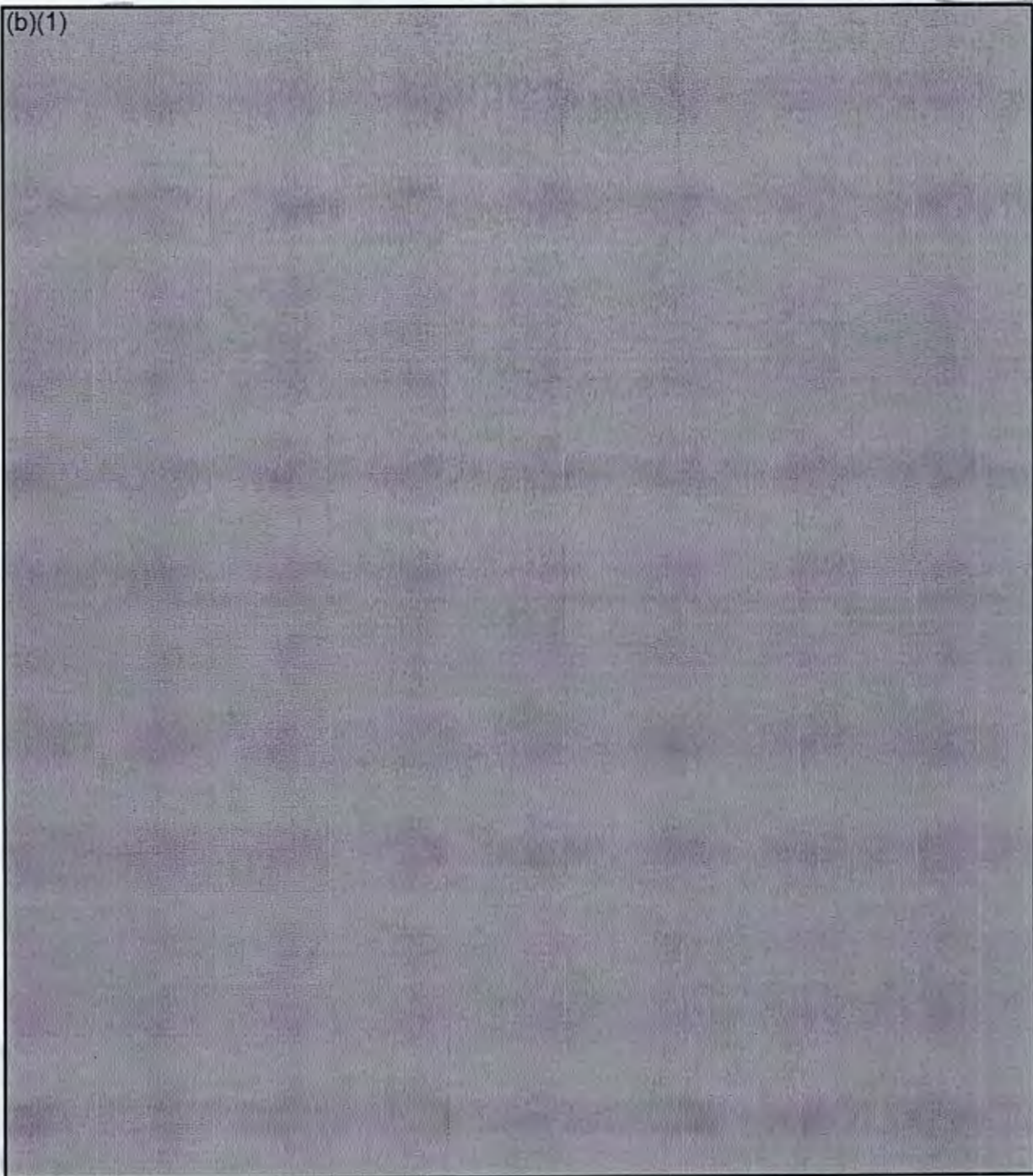
~~TOP SECRET~~

~~TOP SECRET~~

b. (U) The strategic planning process will link defense policy, strategic guidance, and operational planning to ensure coherent effort across the armed forces. Periodic coordination and review will be accomplished at three levels:

(b)(1)

(b)(1)

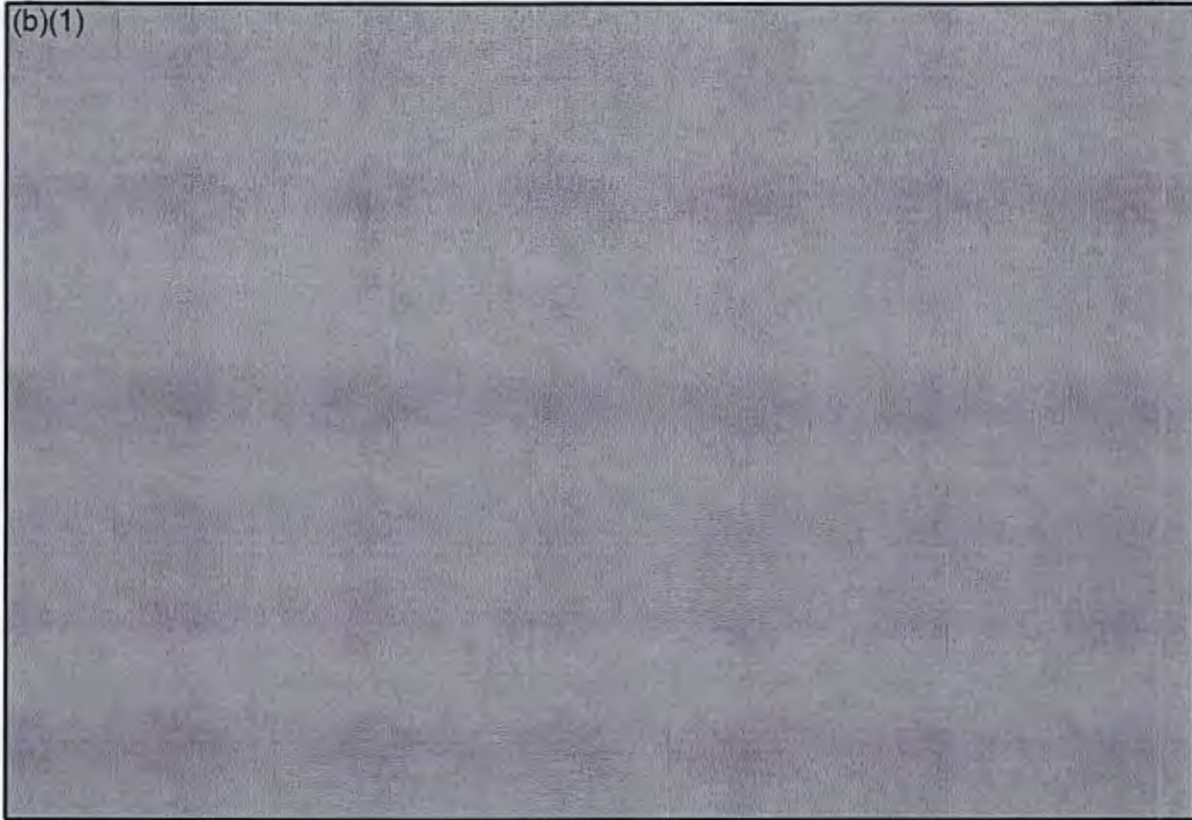


~~TOP SECRET~~

~~TOP SECRET~~

(U)(1)
7

(b)(1)



(4) (U) The Chairman of Joint Chiefs of Staff and the Joint Chiefs of Staff. The Chairman and the Joint Chiefs will assist the Secretary of Defense to provide strategic direction by integrating combatant command perspectives and needs with Service priorities while ensuring consistency with national policy and guidance.

4. (U) Risk Assessments. Risk assessments will be an integral component in each level of periodic review of the global war on terrorism. The NMSP-WOT serves as the basis for these assessments, and updates will be required as strategic conditions evolve. Risk assessments will be conducted in accordance with Joint Staff Notice (JSN) #5641, June 2001, "Procedure for Chairman's Assessment and Assessment of Risk," and will provide the Chairman of the Joint Chiefs of Staff, the Joint Chiefs of Staff, and the Secretary of Defense the information necessary to assess the risk associated with ongoing and planned WOT operations within a global context framed by our other worldwide commitments.

a. (U) Risk Definition and Methodology. Risk, in a general sense, may be defined as the probability of failure to achieve objectives. Assessing risk is fundamentally a subjective process of applying judgments to analyze and draw conclusions from objective data. The process of assessing risk informs decision making, since it gauges the consequences of choices about priorities and the

~~TOP SECRET~~

~~TOP SECRET~~

allocation of resources. The three types of risk outlined by JSN#5641 are military risk, strategic risk, and political risk.:

(1) (U) Military risk is defined as the probability of not achieving established military objectives. It focuses on capabilities and whether they will be adequate to achieve the desired military outcomes. If US forces cannot militarily deter or defeat the forces of its adversaries, then a condition of military risk is created.

(2) (U) Strategic risk is defined as the probability of the Joint Force not achieving the objectives of the National Defense Strategy. It focuses on the ability of the Joint Force to simultaneously achieve the core objectives of the strategy. Strategic risk provides a gauge of the balance among competing objectives, policy choices, commitments involving force employment, the level of resources devoted to each of the objectives, and the tradeoffs resulting from strategic choices.

(3) (U) Political risk is defined as the probability of not achieving the objectives of the National Strategy. It focuses on whether the Joint Force will be able to defend the interests of the Nation when conditions necessitate the use of force. Political risk results from an undesired change in the relative power and influence of the United States. This change can take place with respect to a particular nation, a grouping of nations in a particular region, a particular alliance or coalition, or in the broader international political arena. If the Joint Force is unable to achieve desired military outcomes or honor US commitments to other nations or alliances, then US standing in the broader international political arena is diminished and a condition of political risk is created.

b. (U) Severity of Risk. Severity of risk is assessed to be low, moderate, or high based on the likelihood or probability of failure.

(1) (U) Low risk. The probability of failure to achieve objectives is insignificant. Success in achieving essential military objectives, with capabilities available or projected to be available, is expected.

(2) (U) Moderate risk. The probability of failure is unlikely, yet possible. Success in achieving essential military objectives, with capabilities available or projected to be available, is expected while not assured.

(3) (U) High risk. The probability of failure is significant. Success in achieving essential military objectives, with capabilities available or projected to be available, is not expected without a significant overall increase in capabilities.

~~TOP SECRET~~

~~TOP SECRET~~

c. (U) Risk Factors. Risk factors to consider when implementing and assessing risk for the NMSP-WOT include, but are not limited to:

(1) (U) Over-extension and preservation of freedom of action. Preventing strategic over-extension and preserving our freedom of action may be defined as balancing capabilities WOT and non-WOT-related requirements. We must carefully analyze force commitments and the ability to successfully deter while conducting decisive operations against terrorist organizations and/or their sponsors. Extended commitments of forces in multiple operations may limit our freedom of action or ability to adapt rapidly to changing conditions, opportunities, or emerging threats.

(2) (U) Force Generation and Sustainment. Force generation is the ability to provide ready forces with the capabilities required to perform required missions. The WOT, when combined with our ongoing global security commitments, will stretch and extend military forces. The readiness and sustainment of key capabilities must be considered as WOT operations continue over time. Subcategories include infrastructure; the health and condition of alliances, partnerships, and coalitions; and the ability to maintain our national and international will to continue the WOT.

(3) (U) Military Interoperability. Military interoperability is the ability of the Joint Force to command and control and operate effectively with potential coalition partners.

(4) (U) Interagency Integration and Synchronization. Interagency integration and synchronization enhances military capability by ensuring that other US Government agencies are fully engaged, focused, and organized to provide essential information and support to the Joint Force, during both the planning and execution of WOT operations.

(5) (U) Strategic Mobility. Strategic mobility is strategic sealift, air mobility, ground transportation, mobility infrastructure, and pre-positioned supplies and equipment, both ashore and afloat, that are critical to maintaining strategic agility.

(6) (U) Readiness. Readiness is a current assessment of availability, status of equipment, and manning levels.

(7) (U) Other Factors. Other factors determined by the unique conditions of the theater or AOR, as determined by the commander, may also contribute to risk.

d. (U) Risk Mitigation. In a strategic context, risk mitigation is the ability to identify, isolate, and alleviate sources of potential risk. Mitigating risk

~~TOP SECRET~~

~~TOP SECRET~~

normally involves providing force commanders with significant warfighting improvements and capabilities, to enhance their military advantage, and to preclude adversarial surprises. In the short term, it normally involves adding resources or better aligning mission requirements with the resources that can be made available. Over the long-term, it may involve changes to doctrine, organization, training, materiel, and leadership.

~~TOP SECRET~~

UNCLASSIFIED

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

APPENDIX 1 TO ANNEX H TO THE NATIONAL MILITARY STRATEGIC PLAN
FOR THE WAR ON TERRORISM

ASSESSMENTS

1. Purpose. To provide guidance for unified command and Service assessments of progress on the Strategic Military Objectives for the war on terrorism.
2. General. Combatant commanders and Services are required to submit quarterly assessments of the strategic military objectives for the war on terrorism to the Joint Staff, J-5 (SPC). These inputs form the basis for a continuous assessment of status of prosecution of the war effort and for the development of recommendations for the Joint Chiefs of Staff and the Secretary of Defense to guide further action.
3. Assessment Process. The National Military Strategic Plan for the War on Terrorism (NMSP-WOT) contains seven Strategic Military Objectives and their associated key strategic supporting tasks. Combatant commanders will review the strategic objectives and tasks, develop and/or refine operational tasks to achieve the strategic objective, and assess each objective in accordance with the assessment methodology outlined and distributed via separate cover. The Strategic Planning Team (SPT) will use these assessments to track progress of the war on terrorism, analyze effectiveness of the strategic military objectives, and develop recommendations for the Executive Steering Group (ESG). The ESG will use this information to provide military advice and recommended strategic direction to the Joint Chiefs of Staff and Secretary of Defense.
4. Assessment Format. Format for reporting assessments has been distributed via separate cover. Combatant commanders and Services are provided the option to include comments on specific issues for each of their operational tasks. These comments will be included in a narrative which will accompany the assessment of each strategic military objective. Combatant commanders and Service Chiefs are also requested to provide a "bottom-line" general narrative assessment of their overall status.

UNCLASSIFIED

UNCLASSIFIED

INTENTIONALLY BLANK

UNCLASSIFIED

H-1-2

UNCLASSIFIED

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
WASHINGTON, D.C. 20318
1 October 2002

GLOSSARY TO THE NATIONAL MILITARY STRATEGIC PLAN FOR THE WAR
ON TERRORISM

DEFINITIONS

1. Assure. A range of actions taken both at home and abroad to solidify resolve and demonstrate commitment.
2. Chemical, Biological, Radiological, Nuclear, and High Yield Explosives-Consequence Management (CBRNE-CM). Essential services and activities required to manage or mitigate damages or other consequences or problems resulting from the employment of CBRNE.
3. Civil Support (CS). DOD support to US civil authorities for domestic emergencies and for designated law enforcement and other activities. Referred to as CS. Also see Homeland Security and Homeland Defense definitions.
4. Coalition. An ad hoc arrangement between two or more nations for common action.
5. Compel. A range of actions taken to achieve a change in behavior or activity through the use of all instruments of national power.
6. Consequence Management (CM). Those Department of Defense activities, in support of the US Government lead federal agency, that comprise essential services and activities required to manage or mitigate damages or other consequences or problems resulting from the employment of WMD. This assistance occurs across the spectrum of conflict, ranging from a US Government response to a terrorist incident in the United States to long-term actions necessary to mitigate WMD effects resulting from combat operations.
7. Contain. Efforts taken to limit freedom of action, minimize the effects of terrorist activities, preclude the regeneration of lost capabilities, and/or limit terrorist influence.
8. Critical Infrastructures. Physical and cyber-based systems essential to minimum operations of the economy and government. They include telecommunications, energy, banking and finance, transportation, water systems, and emergency services.

GL-1

UNCLASSIFIED

UNCLASSIFIED

-
9. Defeat. ~~Decisive actions taken to render ineffective, destroy, or eliminate~~ the capabilities of terrorist organizations or their state and nonstate sponsors.
10. Defend. Actions taken to deter, preempt, or prevent attacks against the homeland. Can include conducting preemptive attacks to protect US interests.
11. Destroy. To physically render an entity ineffective or incapable of conducting activity unless it is reconstituted or regenerated.
12. Deter. Actions taken to disrupt, prevent, or preclude acts of aggression. Includes preemptive actions to unhinge the ability to conduct operations.
13. Disrupt. Actions taken to interrupt, temporarily prevent, or desynchronize a terrorist network's capability to conduct operations.
14. Dissuade. The focused application of all elements of national power to convince or persuade an organization, state, or nonstate entity.
15. Homeland Defense (HLD). The protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also see Homeland Security and Civil Support.
16. Homeland Security (HLS). IAW National Strategy for Homeland Security, "Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."
17. Isolate. To separate from a larger whole and set apart, denying freedom of movement and access to external support.
18. Terrorism. Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.
19. Terrorists with global reach - transnational terrorists. Terrorist organizations with an operational and support network in multiple countries that possess the capability to recruit, plan, resource, and execute terrorist acts worldwide.
20. Ungoverned Space. Territory lacking effective, organized, and/or responsible governance, affording secure sanctuary for illicit criminal organizations, terrorist network(s), and antigovernment paramilitaries. Includes under-governed areas within a country with a functioning government.

UNCLASSIFIED

21. ~~Weapons of Mass Destruction (WMD) and/or Weapons of Mass Effects (WMD/E)~~. Weapons that are capable of a high order of casualties, material destruction, or disruption. Weapons of mass destruction/effects can be high-yield conventional explosives as well as nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

GL-3

UNCLASSIFIED

UNCLASSIFIED

INTENTIONALLY BLANK

GL-4

UNCLASSIFIED