

### III. Security Policies

*Doc. No. Description*

- III-1 Secretary Albright and Secretary of Defense Cohen Press Briefing on Land Mine Policy (Demining 2010 Initiative), Washington, October 31, 1997; 5 pp.
- III-2 White House Announcement that U.S. would refrain from using non-self destructing anti-personnel landmines, May 16, 1996, Washington; 2 pp.
- III-3 Presidential Decision Directive 34, New U.S. Conventional Arms Transfer Policy, Washington, February 17, 1995; 9 pp.
- III-4 Department of State Fact Sheet: U.S. Comprehensive Initiative on Small Arms and Illicit Trafficking, Washington, February 23, 2000; 4 pp.
- III-5 Department of State Press Release: U.S. Signs Memorandum with Albania To Destroy Over 130,000 Small Arms/Light Weapons, signed at the Organization for Security and Cooperation in Europe Summit in Istanbul, September 7, 2000; 2 pp
- III-6 White House Press Release: Combatting Terrorism: Presidential Decision Directive 62, Washington, May 22, 1998; 2 pp.
- III-7 White House White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Washington, May 22, 1998; 19 pp.
- III-8 White House White Paper: The Clinton Administration's Policy on Managing Complex Contingency Operations: Presidential Decision Directive 56, Washington, May 1997; 6 pp.
- III-9 Table of Terrorists and outcome of trials
- III-10 Secretary Albright Remarks at Town Hall Meeting on Security, Washington, May 3, 2000; 9 pp.

11-1



Secretary of State Madeleine K. Albright and  
Secretary of Defense William Cohen  
Press Briefing on Land Mine Policy  
Washington, D.C., October 31, 1997  
As released by the Office of the Spokesman  
U.S. Department of State

---

**SECRETARY ALBRIGHT:** Good afternoon. I want to begin by wishing each and every one of you a Happy Halloween.

I am very pleased today to be here with Secretary of Defense William Cohen, to announce a major new United States initiative on a subject of widespread concern in America and around the globe.

The United States is today setting the goal of eliminating the threat posed by land mines to civilians everywhere on the face of the Earth by the end of the next decade.

This call for a concerted effort by the international community is based on the premise that the best way to protect civilians from land mines is to pull mines from the soil like the noxious weeds that they are. There are currently an estimated 100 million mines in more than five dozen countries. At the current rate, we will still be removing mines laid in this century many decades into the next.

The United States is far and away the world's leader in humanitarian demining. Since 1993, we have devoted \$153 million to this purpose. Our experts are helping to remove mines in 14 nations. They have trained and equipped about one quarter of those engaged in demining around the world; and we are continuing to increase our commitment. But still, there is much more that we and others in the international community can and must do.

The President's Initiative, which we are calling "Demining 2010", has several elements:

First, the Administration has asked Assistant Secretary of State Karl F. "Rick" Inderfurth to serve as the new U.S. Special Representative of the President and Secretary of State for Global Humanitarian Demining. Of course, he will also continue in his present job as Assistant Secretary for South Asia, a region that has itself been scarred by the land mine crisis, most tragically in Afghanistan.

Over the past five years, while serving at the US Mission to the UN in New York, Ambassador Inderfurth became a leader in generating international support for efforts to halt the export or transfer of land mines, to establish the goal of their eventual elimination, and to increase demining. He is deeply committed to further progress on these issues and I am grateful for his willingness to take on this new and additional responsibility. Assistant Secretary Inderfurth will be assisted by a deputy, who will be named by the Department of Defense in the days ahead.

The job of the Special Representative will be to work in cooperation with other nations and organizations to coordinate and accelerate international demining efforts, and to increase by

roughly a factor of five--to \$1 billion a year--the public and private resources devoted worldwide to identifying and clearing mines, promoting public awareness about mines, and improving the means of detecting and removing mines.

Second, a panel of distinguished Americans will be appointed to provide advice and help mobilize support for this global initiative. Third, we will host a conference here in Washington to develop specific strategies for achieving the goal of eliminating, by 2010, the threat to civilians posed by land mines already in the ground. A broad cross section of public and private donors, de-miners, recipient nations, NGOs and technical experts will be invited.

Fourth, we will continue to ramp up our own financial commitment to global demining. In 1997, the US Humanitarian Demining Program contributed \$40 million. In 1998, we will contribute close to \$80 million. And we will seek to continue to expand our commitment in 1999 and beyond.

As Secretary of State, I welcome the President's Initiative for several reasons. Accelerating mine clearance will help nations struggling to recover from war to replant their fields, rebuild their economies and re-settle their refugees. It will reduce the long term humanitarian costs of caring for the victims of land mines. It will underline the message that we join with other nations around the world in sending--that it is wrong to endanger civilians through the use of land mines. And above all, it will prevent the killing or maiming of thousands of innocent people every year.

I want to emphasize that the US effort will be conducted in coordination with, not as a substitute for, the work being done by others. We recognize the leadership that has been provided by the United Nations and the commitment that has been made to demining by nations such as Canada, Germany, Norway, South Africa and the United Kingdom. We appreciate the contribution that the Nobel Prize-winning International Campaign to Ban Land Mines has made to increase awareness about the dangers land mines pose. We also respect the Ottawa process and want to continue working with it, although our nation's unique responsibilities for international security have not permitted us to sign the treaty negotiated at Oslo.

In the meantime, Assistant Secretary Inderfurth will be attending the Ottawa Conference in December. We will also ask those in attendance at Ottawa to join us in pushing at the Conference on Disarmament for an immediate, comprehensive and global ban on exports and transfers of anti-personnel land mines.

Thirty-six years ago, President Kennedy set for our nation the goal of enabling a man to walk on the moon. Today, President Clinton is reaffirming the goal of enabling people everywhere to walk safely on the Earth. Together, our nation answered Presidents Kennedy's call. I am confident that together with friends from around the globe, we will achieve President Clinton's vision, as well.

It's now my pleasure to introduce my colleague, Secretary Cohen.

**SECRETARY COHEN:** Thank you very much, Secretary Albright. I am pleased to join with you today to announce this new US initiative to invigorate international efforts to end the humanitarian tragedy of civilians being maimed and killed by land mines. This is the most recent in a series of initiatives through which the United States, under President

Clinton's leadership, has led the world in efforts to eradicate this scourge of humanity.

Over three years ago, President Clinton stepped forward as the first world leader to call for the elimination of anti-personnel land mines. Under the President, the US unilaterally banned the export of these weapons. We have already destroyed 1.5 million of these weapons, and we will destroy another 1.5 million within the next year and a half.

Under President Clinton, the Department of Defense has greatly expanded the humanitarian demining efforts around the world. Secretary of State Albright just mentioned some of these numbers, but let me re-emphasize. We are primarily the country responsible for providing the humanitarian demining assistance to the rest of the world. We provided more than the entire rest of the world combined; all of the nations who have signed, for example, the Ottawa Treaty have not contributed as much combined as the United States has done on its own.

One-quarter of all the active humanitarian deminers in the world were trained by the United States military. There are tangible results that have benefited untold millions - numbers of people - of innocent civilians across the globe have benefited as a result of this. In Namibia, for example, there's been a 90 percent drop in the casualty rate. In Angola, 100,000 people have returned to land that has been cleared of a quarter of a million mines. In Cambodia the land mine death rate has dropped nearly a third. But we believe, as the Secretary said, that much more needs to be done. So today we are launching this new initiative.

What we want is for the other countries to follow the United States' lead: to stop being part of the problem and to start being part of the solution. The United States has stopped and been the leader in stopping being part of the problem. We are the ones who, in fact, have developed systems which do not injure innocent individuals.

Nonetheless, the President went forward beyond our systems which we have spent millions of dollars to develop and said we will eliminate those and go forward with our anti-tank mines, which we believe are absolutely essential to protect our troops. The President made a very principled decision that we need to have force protection for the young men and women, our sons and daughters, who are serving in the military all across the globe. We can do so in a way that nonetheless protects the lives of innocent people all across the globe.

We have been the leader in being part of the solution. What this initiative is, is to ask other countries to join with us in becoming part of the solution, as well. So, Madame Secretary, I'm pleased to be here and we will answer any questions that might come our way.

**QUESTION:** Madame Secretary, it sounds like you're saying that the ban negotiated a month ago really is not the appropriate way to go with this problem and that the way to go is the clearing of mines; is that correct?

**SECRETARY ALBRIGHT:** Well, I think there are two parts to this. I think obviously it is very important to do what we can to ban anti-personnel land mines. We are working on that process, as Secretary Cohen has said, as we have said, through a variety of vehicles. We want to see the Conference on Disarmament take up its appropriate role in this. We are working on getting Congressional treaty ratification of the convention on conventional mine protocol, which will also create some norms on all this.

But we do believe that it's important to work toward the eventual elimination. As Secretary

has said, we have taken a leading role in that, and will continue to do so, commensurate with our responsibilities as the sole superpower, where we have some very special responsibilities. At the same time, we consider that it is absolutely essential to move more robustly in the area of demining because of the hundreds of thousands of mines that are in the ground now that need to be removed, and that we ought to do more in terms of trying to train people to demine, develop new technology so that the demining operations themselves are more sophisticated than what exists now, where basically the tool for demining is a person walking around with one kind of a demining instrument.

**QUESTION:** Secretary Cohen, is there any hope that technology will come to the rescue? We keep hearing about new designs of minefield clearers, new plastic foams. Do you see any hope that that will be a solution?

**SECRETARY COHEN:** Well, we're always looking for technology to help deal with this particular problem. We have a number of research efforts underway - President Clinton, as a matter of fact, has asked for us to develop alternatives, for example, to Korea, where we have mines in place in storage that can be used in specific mine fields. The President has even gone forward, because we have such a clear responsibility to protect our troops there, to see if we can't develop alternatives to those systems currently there.

So we are constantly looking for technology to help deal with force protection, obviously, but also to deal with the humanitarian aspect of this.

**QUESTION:** Off the subject, but I wonder if you'd entertain a question about Iraq, and what has transpired in the 24 hours since the subject last came before someone in the US Government to talk about it. I guess the Iraqis are now saying that while they don't want a conflict, they stand ready for it. I'm wondering if there's anything sub rosa on all of that that you could report to us - any new developments in the stand-off there.

**SECRETARY ALBRIGHT:** Well, let me start, and then perhaps you'll continue. I think that we are obviously concerned about this and we have an approach that we want to take through the United Nations where, in effect, this is an attempt by Saddam Hussein to undercut a very important United Nations approach to this through the monitoring - UNSCOM - through that committee. That is their set-up, as a United Nations instrument, to make sure that the obligations that Iraq has to take up as a result of Security Council resolutions are carried out. It is impossible for Iraq to pick and choose as to who is going to be on this monitoring commission.

There is unanimity among the Security Council members. Many statements have been made about the importance of Saddam Hussein not misinterpreting last week's vote, which was only a tactical difference. There is always the unanimity of the Council about the importance of following up on what UNSCOM needs to do. And that has been made very clear to Saddam Hussein, and I think will continue to be made so through the UN.

**SECRETARY COHEN:** Let me just add to that. The United Nations is not looking for confrontation, but insisting upon compliance. To that extent, the United Nations will insist upon that. As we have indicated before, nothing has been ruled in and nothing ruled out. But we would expect Saddam Hussein to continue complying with the mandates and insist strictly upon that compliance.

**QUESTION:** Have you set any time limit yet to when you might look at this again and do something different than standing and watching and waiting for further response?

**SECRETARY COHEN:** We are carrying on normal operations as we speak. Nothing has changed at this point.

**QUESTION:** One more, slightly off the subject, Madame Secretary, if you would. Do you care to comment on reports of secret meetings between Israel and Syria, under Dennis Ross' auspices here in Washington the last several months?

**SECRETARY ALBRIGHT:** No, I have no comment on that.

**QUESTION:** One more, if I might. Just to clarify if - does the Secretary consider that they are going to try to put new technology to protect the troops. Is that the case for Cuba? I mean, the Guantanamo Base and the Cuban territory has a lot of mines.

**SECRETARY COHEN:** There is in fact every attempt to remove the mines that are not self-destruct types of mines in that area. So those we expect to remove in the near future.

But I should make clear once again that the President has indicated that mixed systems are going to remain in order to provide adequate force protection for forces that are dispersed all across the globe. That's something that the President feels very strongly about - that we in fact need to have the mixed systems for force protection. But our systems are designed in a way that will also promote humanitarian objectives; and that is to not injure innocent women, children, farmers. Our systems will not do that.

[End of Document]

---

[Return to the Secretary's Home Page.](#) [Return to the DOSFAN Home Page.](#)

This is an [official U.S. Government source](#) for information on the WWW. Inclusion of non-U.S. Government links does not imply endorsement of contents.

III-2

The White House  
Current as of: June 24, 1996  
Created May 16, 1996

### U.S. ANNOUNCES ANTI-PERSONNEL LANDMINE POLICY

People in 64 countries, mostly in the developing world, face a daily threat of being killed or maimed by the estimated 100 million landmines in place today. Anti-Personnel Landmines (APL) claim more than 25,000 casualties each year, obstruct economic development and keep refugees from returning to their homeland. As more than a million mines are still being laid each year, they will remain a growing threat to civilian populations for decades unless action is taken now.

The U.S. initiative sets out a concrete path to a global ban on APL but ensures that as the United States pursues this ban, essential U.S. military requirements and commitments to our allies will be protected.

**International Ban**-The United States will aggressively pursue an international agreement to ban use, stockpiling, production, and transfer of anti-personnel landmines with a view to completing the negotiation as soon as possible.

**Korea Exception**-The United States views the security situation on the Korean Peninsula as a unique case and in the negotiation of this agreement will protect our right to use APL there until alternatives become available or the risk of aggression has been removed.

**Ban on Non-Self-Destructing APL**-Effective immediately, the United States will unilaterally undertake not to use, and to place in inactive stockpile status with intent to demilitarize by the end of 1999, all non-self-destructing APL not needed to (a) train personnel engaged in demining and countermine operations, or (b) defend the United States and its allies from armed aggression across the Korean Demilitarized Zone.

**Self-Destructing APL**-Between now and the time an international agreement takes effect, the United States will reserve the option to use self-destructing/self-deactivating APL, subject to the restrictions the United States has accepted in the Convention on Conventional Weapons, in military hostilities to safeguard American lives and hasten the end of fighting.

**Annual Report**-Beginning in 1999, the Chairman of the Joint Chiefs of Staff will submit an annual report to the President and the Secretary of Defense outlining his assessment of whether there remains a military requirement for the exceptions noted above.

**Program to Eliminate**-The President has directed the Secretary of Defense to undertake a program of research, procurement, and other measures needed to eliminate the requirement for these exceptions and to permit both the United States and our allies to end reliance on APL as soon as possible.

**Expanding Demining Efforts-**The Department of Defense will undertake a substantial program to develop improved mine detection and clearing technology and to share this improved technology with the broader international community. The Department of Defense will also significantly expand its humanitarian demining program to train and assist other countries in developing effective demining programs.

III-3

## SECURITY ASSISTANCE LEGISLATION AND POLICY

**New U.S. Conventional Arms Transfer Policy**

[The following is a reprint of Secretary of State message 180317Z Feb 95, subject: Conventional Arms Transfer Policy. This message includes the following: paragraphs 1-3, Department of State comments; paragraph 4, White House Press Secretary Statement of 17 February; paragraph 5, White House Fact Sheet on Conventional Arms Transfer Policy, 17 February; and paragraph 6, White House Fact Sheet on Criteria for Decision-Making on U.S. Arms Exports, 17 February. The final item in this group of documents is a related 17 February press briefing by Eric Newsom, the Principal Deputy Assistant Secretary of State, Bureau of Political-Military Affairs. This is the first release of a formal policy statement on conventional arms transfers since the announcement by the Reagan Administration of its Conventional Arms Transfer Policy on 8 July 1981.]

1. The President recently approved a new policy on conventional arms transfers. This policy will affect future arms transfer issues involving many posts' host governments. Posts are requested to draw on the White House statement and fact sheets in paragraphs 4-6 and present this information to host governments as the Chief of Mission sees appropriate.

2. Introduction—On February 17, the Administration announced its Presidential Decision Directive (PDD-34) on Conventional Arms Transfers. It is the Administration's view as in previous administrations, that sales of conventional weapons are a legitimate instrument of U.S. foreign policy, enabling allies and friends to better defend themselves, as well as help support our defense industrial base. The Administration is determined to ensure a balanced approach, supporting legitimate transfers while restraining those which could threaten our foreign policy and national security interests.

3. At the same time, it is clear that defense exports have important foreign policy and national security implications that differ dramatically from strictly commercial exports.

- PDD-34 should be seen as a summation and codification of this administration's decision-making in the arms transfer arena, rather than a dramatic departure from previous practice. The policy—now in one document—has been reflected in the decisions we have made on arms transfers and efforts at restraint over the past two years.

- While the policy does not represent a radical departure from our historic approach to arms transfers issues, we are giving increased weight—in the changed environment of the post-cold war era—to specific conditions within each region. Just as in our broader defense and non-proliferation strategies, arms transfer policy must be conducted with a focus on the dynamics of regional power balances and the potential for destabilizing changes in those regions.

4. Statement by the White House Press Secretary—Conventional Arms Transfer Policy, February 17, 1995:

The President has approved a comprehensive policy to govern transfers of conventional arms. This policy, as detailed in the attached fact sheets, serves our nation's security in two important ways.

First, it supports transfers that meet the continuing security needs of the United States, its friends, and allies. Second, it restrains arms transfers that may be destabilizing or threatening to regional peace and security.

This policy reflects an approach towards arms transfers that has guided the Administration's decisions over the last two years. Specifically, the United States continues to view transfers of conventional arms as a legitimate instrument of U.S. foreign policy—deserving U. S. government support—when they enable us to help friends and allies deter aggression, promote regional security, and increase interoperability of U.S. forces and allied forces. Judging when a specific transfer will meet that test requires examination of the dynamics of regional power balances and the potential for destabilizing changes in those regions. The criteria guiding those case-by-case examinations are set forth in the attached guidelines for U.S. decisionmaking on conventional arms transfers.

The centerpiece of our efforts to promote multilateral restraint is our initiative to work with allies and friends to establish a successor regime to COCOM [Coordinating Committee for Multilateral Export Controls]. The new regime should establish effective international controls on arms sales and the transfer of sensitive technologies—particularly to regions of tension and to states that pose a threat to international peace and security. While pursuing multilateral restraint through this and other mechanisms such as the UN conventional arms register and regional initiatives, the United States will exercise unilateral restraint in cases where overriding national security or foreign policy interests require us to do so.

#### 5. White House Fact Sheet on Conventional Arms Transfer Policy, February 17, 1995.

U. S. conventional arms transfer policy promotes restraint, both by the U.S. and other suppliers, in transfers of weapons systems that may be destabilizing or dangerous to international peace. At the same time, the policy supports transfers that meet legitimate defense requirements of our friends and allies, in support of our national security and foreign policy interests.

Our record reflects these considerations. U.S. arms sales during this period have been close to our historical average—approximately \$13 billion in government-to-government sales agreements in FY 1994. U.S. arms deliveries have also remained flat. These sales have been primarily to allies and major coalition partners such as NATO member states and Israel.

#### U.S. Goals

The policy issued by the President will serve the following goals:

- 1) To ensure that our military forces can continue to enjoy technological advantages over potential adversaries.
- 2) To help allies and friends deter or defend themselves against aggression, while promoting interoperability with U.S. forces when combined operations are required.
- 3) To promote regional stability in areas critical to U.S. interests, while preventing the proliferation of weapons of mass destruction and their missile delivery systems.
- 4) To promote peaceful conflict resolution and arms control, human rights, democratization, and other U.S. foreign policy objectives.

5) To enhance the ability of the U.S. defense industrial base to meet U. S. defense requirements and maintain long-term military technological superiority at lower costs.

#### Supporting Arms Control and Arms Transfer Restraint

A critical element of U.S. policy is to promote control, restraint, and transparency of arms transfers. To that end, the U.S. will push to increase participation in the UN Register of Conventional Arms. We will also take the lead to expand the Register to include military holdings and procurement through national production, thereby providing a more complete picture of change in a nation's military capabilities each year.

The U.S. will also support regional initiatives to enhance transparency in conventional arms such as those being examined by the OAS [Organization of American States] and ASEAN [Association of Southeast Asian Nations], and will continue to adhere to the London and OSCE [Organization for Security and Cooperation in Europe] guidelines, while promoting adherence to such principles by others.

The United States will continue its efforts to establish a successor export control regime to the Cold-War era COCOM. Our goals for this regime are to increase transparency of transfers of conventional arms and related technology, to establish effective international controls, and to promote restraint—particularly to regions of tension and to states that are likely to pose a threat to international peace and security.

The United States will also continue vigorous support for current arms control and confidence-building efforts to constrain the demand for destabilizing weapons and related technology. The United States recognizes that efforts such as those under way in the Middle East and Europe bolster stability in a variety of ways, ultimately decreasing the demand for arms in these vital regions.

The United States will act unilaterally to restrain the flow of arms in cases where unilateral action is effective or necessitated by overriding national interests. Such restraint would be considered on a case-by-case basis in transfers involving pariah states or where the U.S. has a very substantial lead on weapon technology, where the U.S. restricts exports to preserve its military edge or regional stability, where the U.S. has no fielded countermeasures, or where the transfer of weapons raises issues involving human rights or indiscriminate casualties, such as anti-personnel landmines.

Finally, the U.S. will assist other suppliers to develop effective export control mechanisms to support responsible export policies. The United States will also continue to provide defense conversion assistance to the states of the former Soviet Union and Central Europe as a way of countering growing pressures to export.

#### Supporting Responsible U.S. Transfers

Once an approval for a transfer is made, the U.S. Government will provide support for the proposed U.S. export. In those cases the United States will take such steps as tasking our overseas mission personnel to support overseas marketing efforts of American companies bidding on defense contracts, actively involving senior government officials in promoting sales of particular importance to the United States, and supporting official Department of Defense participation in international air and trade exhibitions when the Secretary of Defense, in accordance with existing law, determines

such participation to be in the national interest and notifies Congress.

## Decision-Making on U.S. Arms Exports: Criteria and Process

Given the complexities of arms transfer decisions and the multiple U.S. interests involved in each arms transfer decision, decisions will continue to be made on a case-by-case basis. These case-by-case reviews will be guided by a set of criteria that draw the appropriate balance between legitimate arms sales to support the national security of our friends and allies, and the need for multilateral restraint against the transfer of arms that would enhance the military capabilities of hostile states or that would undermine stability.

6. White House Fact Sheet on Criteria for Decision-Making on U.S. Arms Exports, February 17, 1994.

Given the complexities of arms transfer decisions and the multiple U.S. interests involved in each arms transfer decision, the U.S. Government will continue to make arms transfer decisions on a case-by-case basis. These case-by-case reviews will be guided by the criteria below.

### General Criteria

All arms transfer decisions will take into account the following criteria:

- Consistency with international agreements and arms control initiatives.
- Appropriateness of the transfer in responding to legitimate U.S. and recipient security needs.
- Consistency with U.S. regional stability interests, especially when considering transfers involving power projection capability or introduction of a system which may foster increased tension or contribute to an arms race.
- The degree to which the transfer supports U.S. strategic and foreign policy interests through increased access and influence, allied burdensharing, and interoperability.
- The impact of the proposed transfer on U.S. capabilities and technological advantage, particularly in protecting sensitive software and hardware design, development, manufacturing, and integration knowledge.
- The impact on U.S. industry and the defense industrial base whether the sale is approved or not.
- The degree of protection afforded sensitive technology and potential for unauthorized third-party transfer, as well as in-country diversion to unauthorized uses.
- The risk of revealing system vulnerabilities and adversely impacting U.S. operational capabilities in the event of compromise.
- The risk of adverse economic, political, or social impact within the recipient nation and the degree to which security needs can be addressed by other means.
- The human rights, terrorism, and proliferation record of the recipient, and the potential for misuse

of the export in question.

- The availability of comparable systems from foreign suppliers.
- The ability of the recipient effectively to field, support, and appropriately employ the requested system in accordance with its intended end-use.

### Upgrade Criteria

Upgrades of equipment—particularly that of former Soviet-bloc manufacture—is a growing segment of the market. The U.S. government should support U.S. firms' participation in that market segment to the extent consistent with our own national security and foreign policy interests. In addition to the above general criteria, the following guidelines will govern U.S. treatment of upgrades :

- Upgrade programs must be well-defined to be considered for approval.
- Upgrades should be consistent with general conventional arms transfer criteria outlined above.
- There will be a presumption of denial of exports to upgrade programs that lead to a capability beyond that which the U.S. would be willing to export directly.
- Careful review of the total scope of proposed upgrade programs is necessary to ensure that U.S. licensing decisions are consistent with U.S. policy on transfers of equivalent new systems.
- U.S. contributions to upgrade programs initiated by foreign prime contractors should be evaluated against the same standard.
- Protection of U.S. technologies must be ensured because of the inherent risk of technology transfer in the integration efforts that typically accompany an upgrade project.
- Upgrades will be subject to standard USG written end use and retransfer assurances by both the integrator and final end user, with strong and specific sanctions in place for those who violate these conditions.
- Benchmarks should be established for upgrades of specific types of systems, to provide a policy baseline against which individual arms transfer proposals can be assessed and proposed departures from the policy must be justified.

## U.S. Conventional Arms Transfer Policy:

### Press Briefing

by

Eric Newsom

Principal Deputy Assistant Secretary of State

Bureau of Political-Military Affairs

As you know, the White House has announced the release of the Administration's policy on conventional arms transfers. I'd like to make a short presentation on the Administration's policy, Presidential Decision Directive (PDD 34).

- The PDD codifies policies that the Administration has been following in this area for the past two years for decisions on individual arms transfers.
- Does not represent a new departure from our current national security and foreign policy goals.

First, the conventional arms transfer policy, defined in PDD-34, is based on two fundamental emphases:

- We seek to promote restraint, both by the U.S. and other suppliers, in transfers of weapons systems that may be destabilizing or dangerous to international peace.
- At the same time, we approve transfers to meet legitimate defense requirements that support our national security and foreign policy interests abroad.
- The Administration's record in the past two years reflects these two emphases.

This policy also is predicated on the reality that the end of the Cold War has not meant the end of dangers to the U.S., or to our interests abroad.

- In this still insecure world, conventional weapons remain legitimate instruments for self-defense and important elements of U.S. national security policy.
- Because not every state can produce the full range of weapons necessary for legitimate defense needs, trade in weapons is inevitable.

Our policy also recognizes that conventional weapons, particularly with the advances of modern technology, can do enormous harm in the hands of hostile states or groups, and appropriate restraint measures can serve our national security interests.

- Unneeded or destabilizing weapons can also exacerbate tensions and place significant economic burdens on some states that seek to obtain and support large militaries.
- These facts argue for continued regulation and restraint in the transfer of weapons and related technology.

Reflecting the continued role of conventional arms transfers for U.S. national security interests, our approach reflects continuity with past arms transfer policy. However, this Administration has given a new emphasis—in its foreign and national security policies—to regional security and stability. Examples:

- Our nonproliferation efforts, which are focused on regions of particular tension;
- Our defense strategy, which is based on planning for two major regional contingencies.

We will be placing the same type of regional emphasis and focus on our conventional arms transfer decisions.

## U.S. Goals

The major goals which our conventional arms transfer policy will serve are:

- 1) Ensuring that our military forces can continue to enjoy technological advantages over potential adversaries.
- 2) Helping allies and friends deter, or defend against, aggression while promoting interoperability with U.S. forces when combined operations are called for.
- 3) Ensuring regional stability in areas critical to U.S. interests while preventing the proliferation of weapons of mass destruction and their missile delivery systems.
- 4) Promoting peaceful conflict resolution and arms control, supporting regional stability, avoiding human rights violations, and promoting other U.S. foreign policy objectives such as the growth of democratic states.
- 5) Supporting the ability of the U.S. defense industrial base to meet U.S. defense requirements and maintain long-term military technological superiority at lower costs.

## The Global Arms Transfer Market

This Administration's record in transfers reflects an understanding of the need for restraint coupled with the realization that transfers to allies and friends bolster our own security. Let me now briefly review basic trends in global arms transfers, to give you the context for our conventional arms transfer policy.

U.S. government arms sales agreements under this Administration have returned to levels below our historical average—approximately \$12 billion a year.

Meanwhile, U.S. arms deliveries have remained basically flat, a trend we expect to continue.

- Sales during this Administration have been primarily to NATO allies and other major friendly states such as Israel.
- U.S. market share has grown not because the U.S. is selling more weapons but because other

suppliers—notably the Soviet Union—have disappeared from the market.

- The global market for arms has also shrunk because domestic procurement budgets have decreased.
- We expect that demand for U.S. arms will remain steady through the remainder of the decade.

The central fact in the international trade in arms is that the global market in conventional arms—measured in deliveries—has declined dramatically.

- Especially notable is the dropoff in sales by the states of the former Soviet Union.
- Over this same period, U.S. conventional arms deliveries stayed relatively steady.

### Arms Transfer Policy Criteria

This Administration will allow a sale only if it meets a set of rigorous criteria. The list is rather long, but some of the most important are:

- consistency with international agreements and arms control initiatives;
- the appropriateness of the transfer as a response to legitimate U.S. and recipient-country security needs;
- the transfer must be consistent with the U.S. interest in regional stability;
- a transfer must afford protection to sensitive technology, as well as protecting against unauthorized transfer to a third party;
- we will examine closely the human rights, terrorism and proliferation-related record of the recipient, and the potential for misuse of the export in question; and
- we will also examine closely the impact of any proposed transfer on U.S. military capabilities, and on the technological advantage enjoyed by U.S. forces.

### Support for U.S. Industry

Our arms transfer decisions will not be driven by commercial considerations. However, once a decision has been made on national security grounds to approve a transfer, it is important that U.S. firms receive the support of this government to make the sale. The Administration will provide the following support to U.S. industry:

- task our overseas mission personnel to support marketing efforts of American companies bidding on defense contracts;
- support official Department of Defense participation in international air and trade exhibitions;
- actively involve senior U.S.G. officials in promoting sales of particular importance to the United States; and

- seek legislation to repeal the statutory requirement to recoup nonrecurring costs on government-to-government sales, and align retransfer restrictions applied to government-to-government sales with those now applicable to commercial sales.

A fundamental point here is that we see support for a strong, sustainable U.S. defense industrial base as a key national security concern of the United States, rather than a purely commercial matter.

Maintaining this industrial base against the uncertainties of future international development is a necessary investment in America's security.

### Arms Control and Restraint

At the same time, a critical part of our policy is the control and restraint of arms and their transfer. We also seek to increase the transparency of arms transfers.

- Restraint and transparency are not ends in themselves.
- They are tools to help reduce mistrust, tension, instability, and ultimately, the destructive cost of conflicts when they occur.

We have made and continue to work on a number of initiatives to establish a new, global pattern of restraint on transfers of conventional arms:

- We will continue to negotiate the COCOM successor regime.
- On transparency, the U.S. will also push to increase participation in the UN Register of Conventional Arms.
- Since the categories of weapons contained in the Register may not be the most relevant to some regional situations, the U.S. will also support regional initiatives to enhance transparency in conventional arms.
- We will also continue to expand our successful programs in export control assistance to Central and Eastern Europe.
- Finally, we will continue our efforts with new emerging suppliers such as South Africa, to provide them with information on how to adopt and apply responsible arms transfer policies.

### Supporting Responsible U.S. Transfers

The U.S. system of reviewing and considering arms transfers is the most rigorous and open in the world.

Arms transfers will continue to be made on a case-by-case basis.

We believe that the Administration's conventional arms transfer policy will achieve all of these goals, in the service of U.S. national security and foreign policy objectives.

III-4



## Washington File

23 February 2000

### **U.S. Comprehensive Initiative on Small Arms and Illicit Trafficking**

This fact sheet was issued 2/15/00 by the U.S. Department of State

The United States is taking a wide range of steps to address growing international concern about trafficking in small arms and light weapons. U.S. efforts are intended to promote regional security, peace and reconciliation in regions of conflict and to make the world safer by helping to shut down illicit arms markets that fuel the violence associated with terrorism and international organized crime.

As Secretary Albright told the United Nations in September 1999, "The international community must develop an integrated, comprehensive response -- in countries of origin and countries of conflict, among buyers, sellers and brokers, and with governments as well as international and non-governmental organizations."

The United States is taking a wide range of steps to address growing international concern about trafficking in small arms and light weapons. U.S. efforts are intended to promote regional security, peace and reconciliation in regions of conflict and to make the world safer by helping to shut down illicit arms markets that fuel the violence associated with terrorism and international organized crime.

As Secretary Albright told the United Nations in September 1999, "The international community must develop an integrated, comprehensive response -- in countries of origin and countries of conflict, among buyers, sellers and brokers, and with governments as well as international and non-governmental organizations." The U.S. contribution to this effort is summarized below.

**OAS Convention Against Illicit Firearms Trafficking.** The United States was a leader in concluding in 1997 the "Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms," the first international agreement designed to prevent, combat, and eradicate illicit trafficking in firearms, ammunition, and explosives. First proposed by Mexico and negotiated in just seven months, this agreement strengthens the ability of the OAS nations to eradicate illicit arms trafficking, while protecting the legal trade in firearms. Key provisions include requiring an effective licensing or authorization system for the import, export, and in-

transit movement of firearms, an obligation to mark firearms indelibly at the time of manufacture and import to help track the sources of illicit guns, and requiring states parties to criminalize the illicit manufacturing of and illicit trafficking in firearms.

**International Protocol Against Illicit Firearms Trafficking.** The United States is working toward completion of the United Nations "Protocol to Combat the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components" by the end of 2000. This protocol would build on and globalize the standards incorporated in the precedent-setting OAS Convention. The protocol is currently under negotiation in the UN Crime Commission in Vienna as part of the negotiations to conclude the Convention Against Transnational Organized Crime.

**Arms Brokering Legislation.** The President signed legislation in 1996 amending the Arms Export Control Act to give the State Department greater authority to monitor and regulate the activities of arms brokers. Cornerstones of the brokering provisions are the requirements that brokers must register with the Department of State, must receive State Department authorization for their brokering activities, and must submit annual reports describing such activities. The United States is one of the few countries to have instituted such legislation, and we are working to promote adoption of similar laws by other nations and to incorporate such a provision into the protocol being negotiated in Vienna. Law enforcement officials made the first seizure of munitions under the provisions of the new legislation in November 1999.

**Greater Accountability.** The United States maintains the world's most open arms export procedures, and is promoting greater openness in the practices of other nations. In 1996, the President signed legislation amending the Foreign Assistance Act of 1961 to require the annual publication of information about arms authorized for commercial export by the United States that fall below the previously existing reporting thresholds for U.S. arms transfers. The report includes detailed, country-by-country information on the numbers of firearms, ammunition, and other "small-ticket" defense items authorized by the United States for export, setting a world standard for transparency. The United States has presented this report as a possible model of transparency to the 33-nation Wassenaar Arrangement, which promotes restraint in the export of conventional arms. The United States also publishes reports on arms flows to regions of conflict in order to raise public awareness of the issue. Last July, for example, the State Department released Arms and Conflict in Africa.

**Careful Scrutiny of Export Licenses.** If arms export license applications exceed the normal, reasonable domestic needs of a given importing country or show other abnormalities, the United States will audit and, if necessary, cut off exports to that country. On that basis, the United States has suspended exports to Paraguay since 1996. In addition, U.S. law prohibits arms and munitions exported from the United States to be re-transferred by the recipient without prior U.S. approval, audits are

conducted if diversions or transshipments are suspected.

**Destroying Excess Weapons.** Helping other nations destroy seized or excess firearms can be an important element in securing a lasting peace in conflict regions. The United States has contributed experts and funds to destroy small arms, light weapons and ammunition in Liberia, Haiti, and the former Yugoslavia. The United States recently agreed with 10 nations of southeast Europe on a program to destroy illicit arms in the region. The United States is also working with the Euro-Atlantic Partnership Council (EAPC), to prevent illicit weapons shipments to the Balkans and central Africa, and to improve security of weapons holdings.

**Cracking Down on Financing of Illicit Arms.** Illicit markets in valuable commodities such as diamonds have helped finance arms flows, particularly to embargoed groups and nations. The United States and other concerned countries are identifying ways to track and intercept illicit trafficking in precious gemstones used in financing conflicts in Africa. One possibility is legislation that would require each diamond to be sold with a certificate of origin guaranteeing its legality. Such an initiative would require continued close cooperation with the diamond industry, whose participation is essential for any dependably effective regime.

**Embargo Enforcement.** The United States carefully observes sanctions and embargoes established by the United Nations. U.S. laws permit the prosecution of those who violate embargoes. We urge others also to criminalize such violations. We recommend that governments find ways to exchange information on violations to truly globalize embargo enforcement. In addition, the United States does not authorize commercial or government-to-government weapons transfers to conflict areas such as the Democratic Republic of the Congo, Ethiopia, Eritrea, and Angola, whose governments are not subject to UN embargoes. We encourage other governments to announce and observe such voluntary moratoria.

**Vigilance at the Borders.** The Administration has made the prevention of illicit arms trafficking across our borders a high priority. The Bureau of Alcohol, Tobacco, and Firearms and the United States Customs Service have intensified their interdiction and investigative efforts. The Attorney General has directed United States Attorneys along the southwest border to make a dedicated effort to prosecute traffickers, large and small, caught attempting to smuggle firearms.

**Africa Focus.** Arms transfers and trafficking and the conflicts they feed are having a devastating impact on Sub-Saharan Africa. Some of the programs we are pursuing, include:

- **Africa Baseline Survey.** Support to the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI) to survey the small arms legislation, regulations, and law enforcement capacities of African countries to provide a benchmark for future work.

- **The West African Small Arms Moratorium.** Technical assistance for the 1998 Economic Community of West African States (ECOWAS) moratorium on the import, export and manufacturing of small arms in West Africa. We are also seeking congressional approval to release modest funding for the moratorium, which was included in the Fiscal 99 Foreign Authorizations Act.

**International Diplomacy.** The United States is working with many nations and international organizations on the problem of illicit small arms.

- **U.S.- EU.** At their December 1999 summit in Washington, the United States and the European Union released a statement of "Common Principles on Small Arms and Light Weapons," in which they pledged to observe the "highest standards of restraint" in their small arms export policies, and took further steps to harmonize their export practices and policies. They approved a 10-point "Action Plan," and established a formal working group through which they will continue their activities.
- **United Nations.** The United States was an active participant and strong supporter of the recommendations of the 1997 Report of the UN Panel of Governmental Experts on Small Arms. The United States will also take active part in preparations for the international conference in 2001 on the "Illicit Arms Trade in All its Aspects."
- **Norway.** The United States has worked closely with a group of like-minded nations led by Norway that is helping to set the international agenda for addressing the problem of small arms proliferation. The statement released by the 18 countries attending the last such conference in Oslo in December 1999 focused special attention on the importance of regulating the activities of arms brokers. President Clinton and Norwegian Prime Minister Bondevik also announced a bilateral task force on small arms and light weapons, focusing on efforts to destroy surplus small arms in conflict zones.

(Distributed by the Office of International Information Programs, U.S. Department of State. Web site: [usinfo.state.gov](http://usinfo.state.gov))

This site is produced and maintained by the U.S. Department of State. Links to other Internet sites should not be construed as an endorsement of the views contained therein.

[back to top](#) ▲

---

[HIP Home](#) | [What's New](#) | [Index to This Site](#) | [Webmaster](#) | [Search This Site](#) | [Archives](#) | [U.S. Department of State](#)

UNCLASSIFIED

III-5



U.S. DEPARTMENT OF STATE

IIP Home | Index to Site | Archives | Search

INTERNATIONAL INFORMATION PROGRAMS

fn. 8

## Washington File

7 September 2000

### Agreement Signed for Destruction of Albanian Small Arms

The United States, Norway, Germany and Albania have signed a memorandum of understanding on the destruction of over 130,000 small arms and light weapons in Albania.

U.S. support for small arms and light weapons destruction in Albania stems originally from work done within the Stability Pact for Southeastern Europe. In a 1999 declaration on small arms and light weapons, Albania, along with nine other countries of Southeastern Europe, committed to the destruction of collected illicit weapons and surplus military stocks.

At the signing of the memorandum of understanding September 7, Assistant Secretary of State Eric Newsom praised Albania, stating that it "will set an example for other countries in the region to deal with the problem of small arms."

*Following is the text of the State Department release:*

**U.S. Department of State  
Washington, D.C.**

**U.S. Signs Memorandum with Albania  
To Destroy Over 130,000 Small Arms/light Weapons**

On September 7, 2000, Assistant Secretary of State for Political-Military Affairs Eric Newsom joined Albania's Minister of Defense, Ilir Gjoni, as well as Norwegian and German diplomats to sign a memorandum of understanding on the destruction of over 130,000 small arms and light weapons in Albania. According to the memorandum, Albania will destroy, with the help of the United States, Norway, and Germany, all weapons collected from the civilian population in the aftermath of the 1997 crisis by the end of 2000. In addition to the 130,000 weapons currently held by the Albanian government, all weapons collected in the future along with surplus military stocks of small arms also will be destroyed.

Albania's small arms problem stems from the crisis of March 1997, during which time nearly 600,000 small arms and light weapons and hundreds of tons of ammunition were looted from government military arsenals around the country. In addition to contributing to a wave of violent crime in Albania, extensive reporting by the United Nations Development Program (UNDP) and independent observers indicates that many of these weapons were smuggled into Kosovo, helping to ignite the conflict there. Since May 1998, the Albania government has bolstered efforts to collect weapons circulating in the civilian population,

UNCLASSIFIED

both through legislation and increased law enforcement measures. This effort was assisted in 1999 by the initiation of a UNDP "Weapons in Exchange for Development" pilot program (originally targeted at the Albanian district of Gramsh, recently extended to Elbasan and Dirba). Under the UNDP program, a limited number of collected weapons have also been destroyed.

U.S. support for small arms and light weapons destruction in Albania stems originally from work done within the Stability Pact. In a November 17, 1999 declaration on small arms and light weapons, Albania, along with nine other countries of Southeastern Europe committed to the destruction of collected illicit weapons and surplus military stocks. The United States and Norway, which have cooperated in supporting small arms destruction efforts globally since the October 15, 1999 Summit between President Clinton and then Prime Minister Bondevik, sent a joint technical assessment team to Albania last May. At the signing of the September 7 Memorandum, Assistant Secretary of State Newsom praised Albania, stating that they "will set an example for other countries in the region to deal with the problem of small arms."

Minister of Defense Ilir Gjoni stated that signing the memorandum "(was) a concrete step that will have an impact first on our daily lives -- we are all conscious of the backlash of these arms in the hands of civilian population, but also because we will offer a concrete example of how we should work to achieve one of the Stability Pact Objectives."

U.S. support for destruction of surplus and illicit small arms and light weapons is intended to promote regional security, peace, and reconciliation in regions of conflict and to make the world safer by helping shut down illicit arms markets that fuel violent insurgent groups, terrorists, and international organized crime.

**(The Washington File is a product of the Office of International Information Programs, U.S. Department of State. Web site: <http://usinfo.state.gov>)**

---

Return to the [Washington File](#)

This site is produced and maintained by the U.S. Department of State. Links to other internet sites should not be construed as an endorsement of the views contained therein.

[back to top](#) ▲

---

[IIP Home](#) | [What's New](#) | [Index to This Site](#) | [Webmaster](#) | [Search This Site](#) | [Archives](#) | [U.S. Department of State](#)

III-6

[CIAO Home Page](#)

[New at the CIAO](#)

[Calendar of Events](#)

[Critical Infrastructure Assurance Summit Meetings](#)

[Congressional Testimony](#)

[National Plan Activities](#)

[Related Links](#)

[CIAO Document Library](#)

[News, Press Releases and Fact Sheets](#)

[Critical Infrastructure Coordination Group](#)

[President's Commission on Critical Infrastructure Protection](#)



Partnership for Critical Infrastructure Security



# Critical Infrastructure Assurance Office

## Combating Terrorism

The following fact sheet on Presidential Decision Directive 62 was released by the White House in May 1998. We have mirrored this release here at the CIAO Web site to facilitate access to information about the directive.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

May 22, 1998

### COMBATING TERRORISM: PRESIDENTIAL DECISION DIRECTIVE 62

Since he took office, President Clinton has made the fight against terrorism a top national security objective. The President has worked to deepen our cooperation with our friends and allies abroad, strengthen law enforcement's counterterrorism tools and improve security on airplanes and at airports. These efforts have paid off as major terrorist attacks have been foiled and more terrorists have been apprehended, tried and given severe prison terms.

Yet America's unrivaled military superiority means that potential enemies -- whether nations or terrorist groups -- that choose to attack us will be more likely to resort to terror instead of conventional military assault. Moreover, easier access to sophisticated technology means that the destructive power available to terrorists is greater than ever. Adversaries may thus be tempted to use unconventional tools, such as weapons of mass destruction, to target our cities and disrupt the operations of our government. They may try to attack our economy and critical infrastructure using advanced computer technology.

President Clinton is determined that in the coming century, we will be capable of deterring and preventing such terrorist attacks. The President is convinced that we must also have the ability to limit the damage and manage the consequences should such an attack occur.

To meet these challenges, President Clinton signed Presidential Decision Directive 62. This Directive creates a new and more systematic approach to fighting the terrorist threat of the next century. It reinforces the mission of the many U.S. agencies charged with roles in defeating terrorism; it also codifies and clarifies their activities in the wide range of U.S. counter-terrorism programs, from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities and protecting the computer-based systems that lie at the heart of America's economy. The Directive will help achieve the President's goal of ensuring that we meet the threat of terrorism in the 21st century with the same rigor that we have met military threats in this century.

### **The National Coordinator**

To achieve this new level of integration in the fight against terror, PDD-62 establishes the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will oversee the broad variety of relevant polices and programs including such areas as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction. The National Coordinator will work within the National Security Council, report to the President through the Assistant to the President for National Security Affairs and produce for him an annual Security Preparedness Report. The National Coordinator will also provide advice regarding budgets for counter-terror programs and coordinate the development of guidelines that might be needed for crisis management.

---

**Contact the CIAO | The Legal Stuff** (*privacy statement, disclaimer, security*)

Page last edited: March 10, 2000

III-7



WHITE PAPER

- President & First Lady
- Vice President & Mrs. Gore
- Record of Progress
- The Briefing Room
- Gateway to Government
- Contacting the White House
- White House for Kids
- White House History
- White House Tours

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

May 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other

- National Security Council Documents
- White Paper: Reforming Multilateral Peace Operations
- White Paper: Managing Complex Contingency Operations
- White Paper: Clinton Administration's Policy; Critical Infrastructure Protection
- NSC Historical List of Policy Documents
- NS Strategy Report: Preface
- International Crime Control Strategy
- NSC Historical List of Meetings with Agenda Topics

natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

## II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems:

## III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical

functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

#### IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council,

shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

## V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.
- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.
- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.
- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.
- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is

achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.
- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.
- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.
- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.
- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

## VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. **Lead Agencies for Sector Liaison:** For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems

related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. **Lead Agencies for Special Functions:** There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.
3. **Interagency Coordination:** The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.
4. **National Infrastructure Assurance Council:** On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel

of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

## VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect

critical infrastructure.

### VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. **Vulnerability Analyses:** For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.
2. **Remedial Plan:** Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.
3. **Warning:** A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.
4. **Response:** A system shall develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.
5. **Reconstitution:** For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.
6. **Education and Awareness:** There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber

systems.

7. **Research and Development:** Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.
8. **Intelligence:** The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.
9. **International Cooperation:** There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.
10. **Legislative and Budgetary Requirements:** There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

## IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition,

following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

### **Annex A: Structure and Organization**

**Lead Agencies:** Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

#### **Lead Agencies for Sector Liaison:**

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

#### **Lead Agencies for Special Functions:**

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence

State	Foreign affairs
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

**National Coordinator:** The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate

analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

### **Warning and Information Centers**

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

**National Infrastructure Protection Center (NIPC):** The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance.

information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD

or the Intelligence Community.

**Information Sharing and Analysis Center (ISAC):**

The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

## Annex B: Additional Taskings

### Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.
- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.
- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.
- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.
- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

### Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection,

the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.
- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.
- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.
- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

#### **Internal Federal Government Actions**

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.
- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and

provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.
- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.
- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.
- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.
- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.
- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.
- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.
- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall

provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

### Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.
- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.
- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

---

[President and First Lady](#) | [Vice President and Mrs. Gore](#)  
[Record of Progress](#) | [The Briefing Room](#)  
[Gateway to Government](#) | [Contacting the White House](#)  
[White House for Kids](#) | [White House History](#)  
[White House Tours](#) | [Help](#) | [Text Only](#)

[Privacy Statement](#)



CRITICAL INFRASTRUCTURE ASSURANCE OFFICE



## Summary of PDD 62 and PDD 63

The following summary of Presidential Decision Directives 62 and 63 was released by the White House in May 1998. We have mirrored this release here at the CIAO Web site to facilitate access to information about these directives.

---

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

May 22, 1998

### SUMMARY OF PRESIDENTIAL DECISION DIRECTIVES 62 and 63

President Clinton today ordered the strengthening of the nation's defenses against emerging unconventional threats to the United States: terrorist acts, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks.

The Combating Terrorism directive (PDD-62) highlights the growing threat of unconventional attacks against the United States. It details a new and more systematic approach to fighting terrorism by bringing a program management approach to U.S. counter-terrorism efforts.

The directive also establishes the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism which will oversee a broad variety of relevant policies and programs including areas such as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction.

The Critical Infrastructure Protection directive (PDD-63) calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. Such infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services. The directive requires immediate federal government action including risk assessment and planning to reduce exposure to attack. It stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives.

For more detailed information on Presidential Decision Directive 63, contact the Critical Infrastructure Assurance Office at (703) 696-9395 for copies of the White Paper on Critical Infrastructure Protection.

III-8

## WHITE PAPER

The Clinton Administration's Policy on Managing Complex Contingency Operations:  
Presidential Decision Directive - 56

May 1997

**Purpose**

This White Paper explains key elements of the Clinton Administration's policy on managing complex contingency operations. This unclassified document is promulgated for use by government officials as a handy reference for interagency planning of future complex contingency operations. Also, it is intended for use in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Regarding this paper's utility as representation of the President's Directive, it contains all the key elements of the original PDD that are needed for effective implementation by agency officials. Therefore, wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government. Note that while this White Paper explains the PDD, it does not override the official PDD.

**Background**

In the wake of the Cold War, attention has focused on a rising number of territorial disputes, armed ethnic conflicts, and civil wars that pose threats to regional and international peace and may be accompanied by natural or manmade disasters which precipitate massive human suffering. We have learned that effective responses to these situations may require multi-dimensional operations composed of such components as political/diplomatic, humanitarian, intelligence, economic development, and security; hence the term complex contingency operations.

The PDD defines "complex contingency operations" as peace operations such as the peace accord implementation operation conducted by NATO in Bosnia (1995-present) and the humanitarian intervention in northern Iraq called Operation Provide Comfort (1991); and foreign humanitarian assistance operations, such as Operation Support Hope in central Africa (1994) and Operation Sea Angel in Bangladesh (1991). Unless otherwise directed, this PDD does not apply to domestic disaster relief or to relatively routine or small-scale operations, nor to military operations conducted in defense of U.S. citizens, territory, or property, including counter-terrorism and hostage-rescue operations and international armed conflict.

In recent situations as diverse as Haiti, Somalia, Northern Iraq, and the former Yugoslavia, the United States has engaged in complex contingency operations in coalition, either under the auspices of an international or regional organization or in ad hoc, temporary coalitions of like-minded states. While never relinquishing the capability to respond unilaterally, the PDD assumes that the U.S. will continue to conduct future operations in coalition whenever possible.

We must also be prepared to manage the humanitarian, economic and political consequences of a technological crisis where chemical, biological, and/or radiological hazards may be present. The occurrence of any one of these dimensions could significantly increase the sensitivity and complexity of a U.S. response to a technological crisis.

In many complex emergencies the appropriate U.S. Government response will incur the involvement of only non-military assets. In some situations, we have learned that military forces can quickly affect the dynamics of the situation and may create the conditions necessary to make significant progress in mitigating or resolving underlying conflict or dispute. However, we have also learned that many aspects of complex emergencies may not be best addressed through military measures. Furthermore, given the level of U.S. interests at stake in most of these situations, we recognize that U.S. forces should not be deployed in an operation indefinitely.

It is essential that the necessary resources be provided to ensure that we are prepared to respond in a robust, effective manner. To foster a durable peace or stability in these situations and to maximize the effect of judicious military deployments, the civilian components of an operation must be integrated closely with the military components.

While agencies of government have developed independent capacities to respond to complex emergencies, military and civilian agencies should operate in a synchronized manner through effective interagency management and the use of special mechanisms to coordinate agency efforts. Integrated planning and effective management of agency operations early on in an operation can avoid delays, reduce pressure on the military to expand its involvement in unplanned ways, and create unity of effort within an operation that is essential for success of the mission.

### **Intent of the PDD**

The need for complex contingency operations is likely to recur in future years, demanding varying degrees of U.S. involvement. The PDD calls for all U.S. Government agencies to institutionalize what we have learned from our recent experiences and to continue the process of improving the planning and management of complex contingency operations. The PDD is designed to ensure that the lessons learned -- including proven planning processes and implementation mechanisms -- will be incorporated into the interagency process on a regular basis. The PDD's intent is to establish these management practices to achieve unity of effort among U.S. Government agencies and international organizations engaged in complex contingency operations. Dedicated mechanisms and integrated planning processes are needed. From our recent experiences, we have learned that these can help to:

- identify appropriate missions and tasks, if any, for U.S. Government agencies in a U.S. Government response;
- develop strategies for early resolution of crises, thereby minimizing the loss of life and establishing the basis for reconciliation and reconstruction;
- accelerate planning and implementation of the civilian aspects of the operation; intensify action on critical funding and personnel requirements early on;
- integrate all components of a U.S. response (civilian, military, police, etc.) at the

- policy level and facilitate the creation of coordination mechanisms at the operational level; and
- rapidly identify issues for senior policy makers and ensure expeditious implementation of decisions.

The PDD requires all agencies to review their legislative and budget authorities for supporting complex contingency operations and, where such authorities are inadequate to fund an agency's mission and operations in complex contingencies, propose legislative and budgetary solutions.

### **Executive Committee**

The PDD calls upon the Deputies Committee to establish appropriate interagency working groups to assist in policy development, planning, and execution of complex contingency operations. Normally, the Deputies Committee will form an Executive Committee (ExCom) with appropriate membership to supervise the day-to-day management of U.S. participation in a complex contingency operation. The ExCom will bring together representatives of all agencies that might participate in the operation, including those not normally part of the NSC structure. When this is the case, both the Deputies Committee and the ExCom will normally be augmented by participating agency representatives. In addition, the chair of the ExCom will normally designate an agency to lead a legal and fiscal advisory sub-group, whose role is to consult with the ExCom to ensure that tasks assigned by the ExCom can be performed by the assigned agencies consistent with legal and fiscal authorities. This ExCom approach has proved useful in clarifying agency responsibilities, strengthening agency accountability, ensuring interagency coordination, and developing policy options for consideration by senior policy makers.

The guiding principle behind the ExCom approach to interagency management is the personal accountability of presidential appointees. Members of the ExCom effectively serve as functional managers for specific elements of the U.S. Government response (e.g., refugees, demobilization, elections, economic assistance, police reform, public information, etc.). They implement the strategies agreed to by senior policy makers in the interagency and report to the ExCom and Deputies Committee on any problems or issues that need to be resolved.

In future complex contingency operations to which the United States contributes substantial resources, the PDD calls upon the Deputies Committee to establish organizational arrangements akin to those of the ExCom approach.

### **The Political-Military Implementation Plan**

The PDD requires that a political-military implementation plan (or "pol-mil plan") be developed as an integrated planning tool for coordinating U.S. government actions in a complex contingency operation. The pol-mil plan will include a comprehensive situation assessment, mission statement, agency objectives, and desired endstate. It will outline an integrated concept of operations to synchronize agency efforts. The plan will identify the primary preparatory issues and tasks for conducting an operation (e.g., congressional consultations, diplomatic efforts, troop recruitment, legal authorities, funding requirements and sources, media coordination, etc.). It will also address major functional

/ mission area tasks (e.g., political mediation / reconciliation, military support, demobilization, humanitarian assistance, police reform, basic public services, economic restoration, human rights monitoring, social reconciliation, public information, etc.). (Annex A contains an illustrative outline of a pol-mil plan.)

With the use of the pol-mil plan, the interagency can implement effective management practices, namely, to centralize planning and decentralize execution during the operation. The desired unity of effort among the various agencies that is created through the use of the pol-mil plan contributes to the overall success of these complex operations.

When a complex contingency operation is contemplated in which the U.S. Government will play a substantial role, the PDD calls upon the Deputies Committee to task the development of a pol-mil plan and assign specific responsibilities to the appropriate ExCom officials.

Each ExCom official will be required to develop their respective part of the plan, which will be fully coordinated among all relevant agencies. This development process will be transparent and analytical, resulting in issues being posed to senior policy makers for resolution. Based on the resulting decisions, the plan will be finalized and widely distributed among relevant agencies.

The PDD also requires that the pol-mil plan include demonstrable milestones and measures of success including detailed planning for the transition of the operation to activities which might be performed by a follow-on operation or by the host government. According to the PDD, the pol-mil plan should be updated as the mission progresses to reflect milestones that are (or are not) met and to incorporate changes in the situation on the ground.

### **Interagency Pol-Mil Plan Rehearsal**

A critical aspect of the planning process will be the interagency rehearsal/review of the pol-mil plan. As outlined in the PDD, this activity involves a rehearsal of the plan's main elements, with the appropriate ExCom official presenting the elements for which he or she is responsible. By simultaneously rehearsing/reviewing all elements of the plan, differences over mission objectives, agency responsibilities, timing/synchronization, and resource allocation can be identified and resolved early, preferably before the operation begins. The interagency rehearsal/review also underscores the accountability of each program manager in implementing their assigned area of responsibility. During execution, regular reviews of the plan ensure that milestones are met and that appropriate adjustments are made.

The PDD calls upon the Deputies Committee to conduct the interagency rehearsal/review of the pol-mil plan. Supporting agency plans are to be presented by ExCom officials before a complex contingency operation is launched (or as early as possible once the operation begins), before a subsequent critical phase during the operation, as major changes in the mission occur, and prior to an operation's termination.

### **After-Action Review**

After the conclusion of each operation in which this planning process is employed, the

PDD directs the ExCom to charter an after-action review involving both those who participated in the operation and Government experts who monitored its execution. This comprehensive assessment of interagency performance will include a review of interagency planning and coordination, (both in Washington and in the field), legal and budgetary difficulties encountered, problems in agency execution, as well as proposed solutions, in order to capture lessons learned and to ensure their dissemination to relevant agencies.

### **Training**

The U.S. Government requires the capacity to prepare agency officials for the responsibilities they will be expected to take on in a planning and managing agency efforts in a complex contingency operation. Creating a cadre of professionals familiar with this integrated planning process will improve the USG's ability to manage future operations.

In the interest of advancing the expertise of government officials, agencies are encouraged to disseminate the **Handbook for Interagency Management of Complex Contingency Operations** published by OASD(S&R) Strategy at (703) 614-0421.

With the support of the State and Defense Departments, the PDD requires the NSC to work with the appropriate U.S. Government educational institutions--including the National Defense University, the National Foreign Affairs Training Center and the Army War College--to develop and conduct an interagency training program. This program, which should be held at least annually, will train mid-level managers (Deputy Assistant Secretary level) in the development and implementation of pol-mil plans for complex contingency operations. Those participating should have an opportunity to interact with expert officials from previous operations to learn what has worked in the past. Also, the PDD calls upon appropriate U.S. government educational institutions to explore the appropriate way to incorporate the pol-mil planning process into their curricula.

### **Agency Review and Implementation**

Finally, the PDD directs each agency to review the adequacy of their agency's structure, legal authorities, budget levels, personnel system, training, and crisis management procedures to insure that we, as a government, are learning from our experiences with complex contingency operations and institutionalizing the lessons learned.

### **Annex A: Illustrative Components of a Political-Military Plan for a Complex Contingency Operation**

- **Situation Assessment**. A comprehensive assessment of the situation to clarify essential information that, in the aggregate, provides a multi-dimensional picture of the crisis.
- **U.S. Interests**. A statement of U.S. interests at stake in the crisis and the requirement to secure those interests.
- **Mission Statement**. A clear statement of the USG's strategic purpose for the operation and the pol-mil mission.

- Objectives. The key civil-military objectives to be accomplished during the operation.
- Desired Pol-Mil End State. The conditions the operation is intended to create before the operation transitions to a follow-on operation and/or terminates.
- Concept of the Operation. A conceptual description of how the various instruments of USG policy will be integrated to get the job done throughout all phases of the operation.
- Lead Agency Responsibilities. An assignment of responsibilities for participating agencies.
- Transition/Exit Strategy. A strategy that is linked to the realization of the end state described above, requiring the integrated efforts of diplomats, military leaders, and relief officials of the USG and the international community.
- Organizational Concept. A schematic of the various organizational structures of the operation, in Washington and in theater, including a description of the chain of authority and associated reporting channels.
- Preparatory Tasks. A layout of specific tasks to be undertaken before the operation begins (congressional consultations, diplomatic efforts, troop recruitment, legal authorities, funding requirements and sources, media coordination, etc.).
- Functional or Mission Area Tasks / Agency Plans. Key operational and support plans written by USG agencies that pertain to critical parts of the operation (e.g., political mediation/reconciliation, military support, demobilization, humanitarian assistance, police reform, basic public services, economic restoration, human rights monitoring, social reconciliation, public information, etc.).

**Extraditions and Renditions of Terrorists  
to the United States  
1993-1999**

<b>Date</b>	<b>Name of Terrorist</b>	<b>Extradition or Rendition</b>	<b>From (Country)</b>	<b>Event</b>
March 1993	Mahmoud Abu Halima	Extradition	Not disclosed	February 1993 World Trade Center bombing
July 1993	Mohammed Ali Rezaq	Rendition	Nigeria	November 1985 Hijacking of Egypt Air 648
February 1995	Ramzi Ahmed Yousef	Extradition	Pakistan	January 1995 Far East bomb plot, February 1993 World Trade Center bombing
April 1995	Abdul Hakim Murad	Rendition	Philippines	January 1995 Far East bomb plot
August 1995	Eyad Mahmoud Ismail Najim	Extradition	Jordan	February 1993 World Trade Center bombing
December 1995	Wali Khan Amin Shah	Rendition	Country not disclosed	January 1995 Far East bomb plot
September 1996	Tsutomu Shiroasaki	Rendition	Country not disclosed	May 1986 attack on US Embassy Jakarta
June 1997	Mir Aimal Kansi	Rendition	Country not disclosed	January 1993 Shooting outside CIA headquarters
June 1998	Mohammed Rashid	Rendition	Country not disclosed	August 1982 Pan Am bombing
August 1998	Mohamed Rashed Daoud Al-Owhali	Rendition	Kenya	August 1998 U.S. Embassy bombing in Kenya
August 1998	Mohamed Sadeek Odeh	Rendition	Kenya	August 1998 U.S. Embassy bombing in Kenya
December 1998	Mamdouh Mahmud Salim	Extradition	Germany	August 1998 East Africa bombings
October 1999	Khalfan Khamis Mohamed	Rendition	South Africa	August 1998 bombing of U.S. Embassy in Tanzania



**Secretary of State Madeleine K. Albright**  
Remarks With Questions and Answers at Town Hall Meeting on  
Security  
Dean Acheson Auditorium  
Washington, DC, May 3, 2000  
As released by the Office of the Spokesman  
U.S. Department of State

---

**SECRETARY ALBRIGHT:** Thank you. Good morning. Good morning to all of you, both here in Washington and those who may be watching overseas. I want to begin by saying "thank you." This is an incredibly busy time for us all. And we are at a pivotal points almost everywhere, from Colombia to China, and from Korea to Kosovo.

This translates into hard work and long hours. For most, the personal and professional pressures are great, the rewards are modest, the victories rarely final. And in many overseas posts, there are often other hardships, including risks to life and limb.

But this is the nature of the business we have chosen -- American foreign policy -- and I feel incredibly privileged to have the opportunity with you to represent our country around the world. In fact, I am jealous that many of you will get to do this for your whole careers, while I will not -- at least not in government service. You are the real custodians of our foreign policy.

When I travel now, I am often asked whether there will be major changes in policy after the November election. And I reply that, of course there will be some changes, whichever party wins, but our fundamental direction is unlikely to shift very much. Overall, there will be continuity, due in large measure to the experience and wisdom provided by you, our Foreign Service, Civil Service and Foreign Service National personnel.

But I didn't come here this morning just to thank you. I also want to discuss with you two issues that have concerned me since the day I took office. The first is resources. America has the world's largest and strongest economy. We are the only country whose interests and capabilities are truly global. And yet, due to a shortage of resources, we are not able to do nearly as much as we should to shape the political and security environment of the 21st Century. This is a potentially tragic error.

When adequately funded, our diplomacy is a remarkable tool for preserving peace, preventing crises, promoting prosperity and providing the answer to global threats. In any rational system of priorities, we would have more to invest in programs, and far more to invest in recruiting, training, equipping, and protecting those who work in our diplomatic posts.

This is why we have launched a strong effort within the Administration, on Capitol Hill and in the country to explain how what we do here at the Department has direct and beneficial impact on the lives of our citizens. We have greatly expanded our educational outreach to key constituency groups. And we have made some headway.

International affairs has been a significant priority in endgame budget negotiations the past two years. Most of our 1998 and 1999 supplemental requests have been honored. Our personnel accounts have stabilized. We are going ahead, although still not as rapidly as we should, with construction and repairs overseas.

Still, like Sisyphus, we have to keep rolling the stone up the hill. This year, Congress passed a budget resolution that would slash twelve percent from the President's request. And our emergency supplemental requests for Colombia and Kosovo and other urgent needs have not been approved.

In my testimony this year, I have repeatedly made the point that most of the funds we are requesting for Fiscal Year 2001 will be spent next year, under a new Administration. So our requests have nothing to do with political parties or individual personalities. Their sole purpose is to advance the interests and values of the United States.

And I pledge to you today that as long as I am Secretary of State, I will fight for our budget; and that as long as I draw breath, I will do all I can to help you get the resources you need to do your jobs well, and thereby keep America secure, prosperous and strong.

The second and main topic I want to discuss will come as no surprise; that is security. In 1997, when I arrived on the 7th floor, coming from New York where I was a chief of mission, I was concerned generally about our security procedures and I also wanted to enhance the morale of our security personnel, improve recruitment, and increase resources. To head this effort, we brought in David Carpenter, the first career law enforcement officer ever to lead the Diplomatic Security Bureau.

Spurred especially by the tragic embassy bombings in 1998, I think we have made real progress. We developed a global risk management plan, enhanced perimeter security, hired more guards, adopted a rigorous escort policy, strengthened computer protections, provided hundreds of security briefings, and began a new surveillance detection program at most posts.

More recently, I asked Assistant Secretary Carpenter to conduct a top-to-bottom review of the Department's security practices. This review was assisted by experts from the CIA, DOD, FBI and Secret Service, and is almost complete. I have also asked the Assistant Secretary to serve as my special adviser on security affairs, while we work with Congress to establish the position of Under Secretary for Security, Counter-terrorism and Law Enforcement Affairs.

I will be frank and say that some of these reforms have been resisted. Today, I want to make it clear that I am asking for, and expect, your full support.

Because we cannot and should not accept a culture within the Department that resists paying full attention to our security responsibilities. We cannot and should not suggest that those responsibilities somehow interfere with the performance of our jobs. For, in truth, this is not possible. Security is an inherent, inextricable, and indispensable component of all our jobs.

As you well know, a laptop computer containing sensitive information disappeared recently from one of the most secure areas of the Department. Combined with the 7th floor bugging incident, this demonstrates that more efforts on our part are needed. And these events have raised questions within Congress and the public about our commitment to security.

You may have seen reports indicating that I am furious about these incidents. Well, I am, and hope you are, too. Failures to observe basic procedures put our nation's secrets at risk. They damage the credibility and reputation of the Department and everyone who works here. They are intolerable and inexcusable. And together, we must strive to make their repetition unimaginable.

Let me stress a few points. First, I repeat: security is a core component of the job of each and every person in this room, and those listening to us outside. I don't care how skilled you are as a diplomat, how brilliant you may be at meetings, or how creative you are as an administrator; if you are not professional about security, you are a failure.

Every personnel review should include an evaluation of how well security-related responsibilities are fulfilled. And every employee who handles or safeguards classified or sensitive information must attend the Department's annual security briefings. Getting security right requires not just a short burst of attention. It demands a permanent commitment.

Second, the vast majority of State Department employees already take their security duties very seriously. I can't emphasize that enough. It is the few who neglect or who are casual about their duties who create problems for all of us. So this is one area where we must each be our neighbor's keeper. If you see a violation, don't look the other way. Correct it, report it, and ensure it doesn't happen again.

Third, forget that the Cold War ended. Spy novelists may be having trouble thinking up plots, but our nation still has enemies; our secrets still need protecting; and the threats we face are more varied and less predictable than ever. Jefferson had it right when he said that liberty's price is "eternal vigilance."

Fourth, don't let where you serve affect the precautions you take. It may seem less necessary to go the extra mile for security here than in a sensitive overseas post. It is not. The imperatives of day-to-day security do not change whether you live in Bethesda or Beijing.

Finally, don't rely on memory alone. Develop and follow procedures. I have to tell you that when I fly on a plane that says the United States of America, with our trained pilots who have flown thousands of hours, and I watch them in the cockpit, they sit there with a manual and they go through every step by step, making sure that they do the right things in flipping switches and moving various gidgets around. And I am so impressed at the discipline that they take in doing that. And they do it because they don't want to go down. And we don't want to go down either. We should do the same kind of procedures every day before we go home.

Let me emphasize again that, in responding to this challenge, there is no "us" or

"them", only "we". We all have an interest in seeing that those who need highly sensitive information in their jobs have access to it, on a convenient and timely basis. We all have an interest in guaranteeing the security of that information, for without that guarantee, the information will be compromised and access to similar data in the future will be in doubt.

We all have a stake in safeguarding the interests of our nation, and in seeing that within our Department, there exists a climate and culture which ensures that security is a top priority for every employee, every day. This is essential to the future of the US Department of State, and critical, therefore, to the future our country, because American diplomacy is our first line of defense, and together, we have vital work to do on behalf of democracy, in support of peace, in service to our citizens, and in fulfillment of our nation's unique global role.

I have never been prouder than to serve with all of you. And I am confident that we will respond appropriately now, and proceed with America's work at a level of excellence unmatched by any comparable institution anywhere in the world.

Thank you very much, and I'll now be happy to take your questions.

(Applause.)

**QUESTION:** Good morning, Madame Secretary. My name is Gary Galloway and I'm proud to serve as Agency Vice President for the American Federation of Government Employees, representing more than 6,000 bargaining unit employees in the Department.

It's been our experience that, in the past, when security violations have been observed by civil service employees, reporting of these violations has resulted, in some cases, in no action -- and, in the worst cases, retaliation or reprisal against employees.

What we would like to know is what new measures will be taken to ensure that these issues will be addressed without negative consequences to employees.

**SECRETARY ALBRIGHT:** Well, first of all, let me say that what is very important is that we all understand this is a responsibility for everybody equally -- Foreign Service, Civil Service and Foreign Service nationals, as I have said. And that what has to happen, we have to understand that we all have a joint responsibility for this and no one's career will suffer unjustly and no one's, on this most recent incident, has. People have been moved but their investigation is ongoing.

And I believe that the procedures that will be in place will be such that people will be treated fairly, that their rights will be respected, and that no one will be in any way demeaned or punished for something before there is a full investigation. I do think it is important, however, that we take the kinds of measures immediately that make it possible for investigations to go forward.

**QUESTION:** Madame Secretary, Marshall Adair, President of the American Foreign Service Association.

First of all, I would like to commend you for your work on this issue, not only the issue of security of information, but also security of personnel. Both of them we recognize are critical to the management of effective foreign policy.

I think that we also -- we need to point out that information of security overall has been managed very well, particularly at our overseas posts. It is more difficult here at the Department of State. The challenge is substantially more difficult. It is a larger institution, it is more diverse and it also has a commitment, reinforced by this Administration, correctly so, to maintain openness to the public. That makes things far more difficult.

As you pursue your efforts to improve security here at the Department of State, I am sure that the Foreign Service and certainly the Foreign Service Association will work very hard together with you. We would appeal -- we would make several appeals to you, however.

First of all, that you concentrate resources on security problem itself and not be diverted by responding to the critics, as opposed to the problem. Secondly, do as you have just done today: Seek the cooperation of those working here, rather than seeking to apportion blame. And, third, seek more resources. And I would commend you for your comments today in that regard and certainly for your efforts over the last several years to improve the foreign affairs budget here, because we can't do anything without more resources. The budget of the Department of State right now is appallingly low.

As I say, we will certainly work with you in this regard. My question here would be: Have you made an estimate now of the kinds of resources it will take to substantially improve this kind of security at the Department of State?

**SECRETARY ALBRIGHT:** First of all, thank you very much for your words of support and your understanding that we are all in this together. I feel that very strongly and, as I look around this room and see the many people that I have had contact with, whether it's in my office or in the cafeteria, you are all amazing people who are incredibly dedicated to this country. And, as I have said, I am very grateful for the privilege of serving with you.

But I think what we have to understand is how serious this is and how one, in fact, balances what you said, Marshall, about the openness of our society and our need to carry on work.. And we are going to try to find that balance.

Dave Carpenter, as I said, is going through this top-to-bottom and bottom-to-top review with his other law enforcement colleagues. He has given me a preliminary report, but we haven't done yet the assessment on the resources.

Where we have a problem is when I've gone to testify -- and we are increasingly conscious of security issues because of the terrible bombings -- of how not to have -- and this is more of a building issue -- how not to have just secure buildings with nobody in them with no programs, or people who are exposed in places, and I've just visited some really miserable locations where our embassies, the structures themselves, where they are located, where they have programs and they are not

secure.

So we are working with Congress and with each other to try to develop a good balance. But I do think that we are in an unfortunate era where we have to be much, much more concerned about security, as I said in my remarks, as a core issue. But we are working on the balance and Dave is working on providing me with estimates of resources that we will need and also outlining the various procedures that have to happen here in terms of going to the security reviews and having people come into each part of the Department to go over the security procedures, making sure that the right people are working on the problem, and that it really is a responsibility of everyone.

All I can do is give you a kind of home analogy. Everybody, when they leave a house, is responsible for locking the door. It isn't up to just one member whose job it is to lock the door. And that is where we have to act together.

**QUESTION:** Good morning. My name is Karen Saxe, I am a regional computer security officer in charge of the United States, Canada and the NEA, one of two. And I want to say thank you for your strong words of support for security. We appreciate it greatly. We can use it with our briefings with ambassadors, posts, bureaus and so forth.

I did have a question. This is more computer security related, given the issue with the INR laptop and because that concerns me personally. Domestically, and I know you just are beginning to work with the Under Secretary for Security, domestically with computer security issues, have you given any thought to strengthening domestic policy for computer security? We're very weak in that area. Any work in that area would be of great use to us to help us when we go and do evaluations of bureaus and such to be able to have something to stand on to say to people that this isn't secure for this reason and you should do these things. Right now, we don't have that backing.

**SECRETARY ALBRIGHT:** Absolutely. Let me just make the following point. I think this is not true of everyone in this room, but I think we are all into a new technology era where -- we were saying this the other day -- that if, in fact, there had been 5,000 pieces of paper on a desk and they disappeared, you'd kind of be aware of the fact that they were gone. And especially if they were marked with all the appropriate markings.

And the problem here is that, as computer literate as many people are, they still don't, I think, fully understand what it is that happens with a laptop computer and hard drives and CD-ROMs and various aspects of them. And I think that we just need to be better about understanding.

Yesterday, I was with the Wall Street Journal Editorial Board and they were, as you can imagine, asking me about this. And I think that it is a question of technology and how people understand and handle it. And you will have, as a result of the procedures that we're setting up, a much more specific set of guidelines that I think will help you in order for the rest of the people here to understand the security and sanctity of a laptop or any computer, given the transfer of information that way.

**QUESTION:** Bruce Matthews. I am a security engineering officer with our Diplomatic Security Training Center at the moment. I, too, appreciate your comments. I am already lamenting the fact that many of our colleagues will read them only in words on paper. I don't think they can appreciate the honesty with which you delivered them. I do appreciate that.

**SECRETARY ALBRIGHT:** We'll make a video.

(Laughter.)

**QUESTION:** There you go. Modern technology helps.

I do have an appeal, though. I think one of the issues that we need to deal with fundamentally in the Department is our lack of classification guidelines. It is hard to hold anyone accountable or have an accountability structure that's effective without something to state when that accountability needs to be put in place. And other agencies do have classification guidelines and, to my knowledge, we don't have a well-established set within the Department to the detail required for the average user who's writing and creating documents and material to have a solid guidance of when they should classify and to what level.

And so my appeal to you is to start an effort, if we can, to either better publish them if they exist or to create them if they don't.

**SECRETARY ALBRIGHT:** I think you have a very important point and I think that there are a lot of people who actually believe that documents are over-classified or they are classified incorrectly, and kind of a sense that if a cable comes in classified, that the response also has to be classified, and a number of questions that people have. I think that this is an issue that also does need clarification and will be clarified, because it's an important part of the process.

Let me say that, you know, I do not in any way wish to underestimate what has happened here: it is huge and terrible. But I hope that we can use this not only as something that has made us realize the importance of what we're doing but to turn it into a good learning lesson about questions such as you're raising, where people kind of go along with what they think is the process without fully understanding it. And so we are going to look at not only what you asked about the guidelines for computers, but just how to do things better. And Dave is going to work on that and, Skip, you are going to get involved in a lot of these aspects.

And I must say that we're getting tremendously good cooperation from the Agency and Director Tenet and I have been talking and will continue to talk about how to improve various parts of this. And I think people -- Ambassador Gnehm has told me that you all have cards and things that we hope very much that you will not only have questions on that we can answer later but also suggestions and things that you believe ought to be looked at.

I can't emphasize enough the "we" part of this. I feel very strongly about this, as is evident, but I can't do this alone. I am the ultimate person that is responsible for this and I take that responsibility on. But all of you have to be a part of this, and I think

suggestions of various kinds will be very helpful.

**QUESTION:** Madame Secretary, my name is Kerri Eggspuehler and I am a computer security specialist with Diplomatic Security. And one of the things that Assistant Secretary Carpenter has been very supportive of is our efforts in computer security. And we travel on teams that do assessments of our computer systems worldwide. And one of the things that I think has not been addressed is that our upper level management -- first of all, many times when I brief an ambassador, a DCM or a consulate general, they tell me this is the first time they've ever had a computer security briefing in their entire careers. And many times, you know, they're very upset about this.

But I have also been confronted with senior management who basically say, I don't have to deal with this, this isn't my problem. And a lot of times, computer security or any security is going to come from the top down. So I appreciate your comments on this, and I was wondering how we are going to educate our senior management to take this seriously and to recognize it, because it's not just a matter of, you know, the individuals doing it but really our senior management making a commitment to this.

**SECRETARY ALBRIGHT:** I believe we all have to make that commitment. And it's a little bit -- I think it may be that some of the senior people are embarrassed to admit that they don't know anything about it, you know. So people should feel free to ask all the questions they always wanted to know about computers. And, you know, it's a generation problem, I can assure you.

(Laughter.)

But I think that we need to do that, and people should not be embarrassed to figure out how to even turn on their computer. So I urge everybody and Dave is working. We are going to have a program here that requires people to go to various sessions, where all of you will be going around even on a more frequent basis to make these kinds of explanations. And if people want to talk to you privately, they can do that. But I really do believe that you're absolutely right: it has to come from the top down.

**QUESTION:** I mean, this is twofold. I mean, when you were talking earlier about accountability, because that's one of the things, too. We've briefed literally almost 10,000 people in the last two years. But it's one of those things that, if they aren't held accountable for their actions, then why do we even do the work that we do? And the gentleman that first that was speaking was saying, you know, I hope careers aren't influenced by this. But I think they should be, if they have flagrant disregard for security in every aspect. So I think accountability is a key issue and part of that.

**SECRETARY ALBRIGHT:** I agree with that. Which is why, in my remarks, I said that as there are evaluations are being made of people as to whether they are performing their jobs well, how they are accountable on security issues is going to be a part of that. I think that that is essential. And I must say, I am very glad you raised the question of accountability. There is a little bit too much of this going on, and "I didn't see it" or "I didn't do it" or "It wasn't my responsibility." And this goes back to, you know, everybody is responsible for locking the front door.

I think people in a bureaucracy, any bureaucracy, have a tendency to say somebody else did it. And we can't have that kind of culture. I'm kind of -- you know, I was calling members of Congress up about this, which was not a great, fun activity -- (laughter) -- and some of them said, well, it's just the culture of the State Department. That's embarrassing. I don't want to answer for that. I don't want to be humiliated or embarrassed on our behalf. I want to be proud, as we justly should be, of many -- all, mostly -- fantastic people here. And you have to take accountability. And you're absolutely right.

Thank you all very much.

[End of Document]

---

[Secretary's Home Page](#) | [State Department Home Page](#)

## Documentary Annexes

### IV. Arms Control

*Doc. No. Description*

- IV-1 Decision of the States Party to the Treaty on the Non-Proliferation of Nuclear Weapons: Strengthening the Review Process for the Non-Proliferation Treaty, New York, May 12, 1995; 1 p.
- IV-2 Decision of the States Party to the Treaty on the Non-Proliferation of Nuclear Weapons: Principles and Objectives for Nuclear Non-Proliferation and Disarmament, New York, May 12, 1995; 4 pp.
- IV-3 Decision of the States Party to the Treaty on the Non-Proliferation of Nuclear Weapons: Extension of the Treaty on the Non-Proliferation of Nuclear Weapons, New York, May 12, 1995; 1 p.
- IV-4 White House Press Release: Joint Statement Concerning Management and Disposition of Weapon-Grade Plutonium Designated as No Longer Required for Defense Purposes and Related Cooperation, Moscow, June 4, 2000; 1 p.
- IV-5 Joint Statement of the United States and the People's Republic of China: Missile Proliferation, Washington, October 4, 1994; 1 p.
- IV-6 Department of State Fact Sheet: Joint United States-People's Republic of China Statement: Missile Proliferation and Joint United States-People's Republic of China Statement on Stopping Production of Fissile Materials for Nuclear Weapons, Washington, October 4, 1994; 3 pp.
- IV-7 Joint Statement by President Clinton and President Putin: Strategic Stability Cooperation Initiative, New York, September 6, 2000; 4 pp.
- IV-8 White House Press Release: Joint United States-Russian Statement on Parameters on Future Reductions in Nuclear Forces, Helsinki, March 21, 1997; 2 pp.
- IV-9 White House Press Release: Joint Statement by President Clinton and President Yeltsin: Anti-Ballistic Missile Treaty, Helsinki, March 21, 1997; 3 pp.
- IV-10 White House Press Release: Joint Statement between the United States and the Russian Federation Concerning Strategic Offensive and Defensive Arms and Further Strengthening of Stability, Cologne, Germany, June 20, 1999; 2 pp.
- IV-11 Letter from President Clinton to the Senate of the United States transmitting for advice and consent to ratification the Comprehensive Nuclear Test-Ban Treaty, Washington, September 22, 1997; 6 pp.

- IV-12 Letter from President Clinton to the Senate of the United States transmitting for advice and consent to ratification the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Washington, November 23, 1993; 19 pp. including attachments.
- IV-13 White House Press Release: Remarks by President Clinton on National Missile Defense, Georgetown University, Washington, September 1, 2000; 7 pp.

Created December 9, 1996

IV-1

New York, 17 April-12 May 1995

NPT/CONF.1995/32/DEC.1

Decision**STRENGTHENING THE REVIEW PROCESS FOR THE TREATY**

1. The Conference examined the implementation of article VIII,3, of the Treaty and agreed to strengthen the review process for the operation of the Treaty with a view to assuring that the purposes of the Preamble and the provisions of the Treaty are being realized.
2. The States party to the Treaty participating in the Conference decided, in accordance with article VIII,3, of the Treaty, that Review Conferences should continue to be held every five years and that, accordingly, the next Review Conference should be held in the year 2000.
3. The Conference decided that, beginning in 1997, the Preparatory Committee should hold, normally for a duration of 10 working days, a meeting in each of the three years prior to the Review Conference. If necessary, a fourth preparatory meeting may be held in the year of the Conference.
4. The purpose of the Preparatory Committee meetings would be to consider principles, objectives and ways in order to promote the full implementation of the Treaty, as well as its universality, and to make recommendations thereon to the Review Conference. These include those identified in the Decision on Principles and Objectives for Nuclear Non-Proliferation and Disarmament adopted on 11 May 1995. These meetings should also make the procedural preparations for the next Review Conference.
5. The Conference also concluded that the present structure of three Main Committees should continue and the question of an overlap of issues being discussed in more than one Committee should be resolved in the General Committee, which would coordinate the work of the Committees so that the substantive responsibility for the preparation of the report with respect to each specific issue is undertaken in only one Committee.
6. It was also agreed that subsidiary bodies could be established within the respective Main Committees for specific issues relevant to the Treaty, so as to provide for a focused considered of such issues. The establishment of such subsidiary bodies would be recommended by the Preparatory Committee for each Review Conference in relation to the specific objectives of the Review Conference.
7. The Conference agreed further that Review Conferences should look forward as well as back. They should evaluate the results of the period they are reviewing, including the implementation of undertakings of the States parties under the Treaty, and identify the areas in which, and the means through which, further progress should be sought in the future. Review Conferences should also address specifically what might be done to strengthen the implementation of the Treaty and to achieve its universality.

IV-2

Created December 9, 1996

New York, 17 April-12 May 1995

NPT/CONF.1995/32/DEC.2

Decision**PRINCIPLES AND OBJECTIVES FOR NUCLEAR  
NON-PROLIFERATION  
AND DISARMAMENT**

Reaffirming the preamble and articles of the Treaty on the Non-Proliferation of Nuclear Weapons,

Welcoming the end of the cold war, the ensuing easing of international tension and the strengthening of trust between States,

Desiring a set of principles and objectives in accordance with which nuclear non-proliferation, nuclear disarmament and international cooperation in the peaceful uses of nuclear energy should be vigorously pursued and progress, achievements and shortcomings evaluated periodically within the review process provided for in article VIII (3) of the Treaty, the enhancement and strengthening of which is welcomed,

Reiterating the ultimate goals of the complete elimination of nuclear weapons and a treaty on general and complete disarmament under strict and effective international control,

The Conference affirms the need to continue to move with determination towards the full realization and effective implementation of the provisions of the Treaty, and accordingly adopts the following principles and objectives:

Universality

1. Universal adherence to the Treaty on the Non-Proliferation of Nuclear Weapons is an urgent priority. All States not yet party to the Treaty are called upon to accede to the Treaty at the earliest date, particularly those States that operate unsafeguarded nuclear facilities. Every effort should be made by all States parties to achieve this objective.

Non-proliferation

2. The proliferation of nuclear weapons would seriously increase the danger of nuclear war. The Treaty on the Non-Proliferation of Nuclear Weapons has a vital role to play in preventing the proliferation of nuclear weapons. Every effort should be made to implement the Treaty in all its aspects to prevent the proliferation of nuclear weapons and other nuclear explosive devices, without hampering the peaceful uses of nuclear energy by States parties to the Treaty.

Nuclear disarmament

3. Nuclear disarmament is substantially facilitated by the easing of international tension and the strengthening of trust between States which have prevailed following the end of the cold war. The undertakings with regard to nuclear disarmament as set out in the Treaty on the Non-Proliferation of Nuclear Weapons should thus be fulfilled with determination. In this regard, the nuclear-weapon States reaffirm their commitment, as stated in article VI, to

pursue in good faith negotiations on effective measures relating to nuclear disarmament.

4. The achievement of the following measures is important in the full realization and effective implementation of article VI, including the programme of action as reflected below:

(a) The completion by the Conference on Disarmament of the negotiations on a universal and internationally and effectively verifiable Comprehensive Nuclear-Test-Ban Treaty no later than 1996. Pending the entry into force of a Comprehensive Test-Ban Treaty, the nuclear-weapon States should exercise utmost restraint;

(b) The immediate commencement and early conclusion of negotiations on a non-discriminatory and universally applicable convention banning the production of fissile material for nuclear weapons or other nuclear explosive devices, in accordance with the statement of the Special Coordinator of the Conference on Disarmament and the mandate contained therein;

(c) The determined pursuit by the nuclear-weapon States of systematic and progressive efforts to reduce nuclear weapons globally, with the ultimate goals of eliminating those weapons, and by all States of general and complete disarmament under strict and effective international control.

#### Nuclear-weapon-free zones

5. The conviction that the establishment of internationally recognized nuclear-weapon-free zones, on the basis of arrangements freely arrived at among the States of the region concerned, enhances global and regional peace and security is reaffirmed.

6. The development of nuclear-weapon-free zones, especially in regions of tension, such as in the Middle East, as well as the establishment of zones free of all weapons of mass destruction should be encouraged as a matter of priority, taking into account the specific characteristics of each region. The establishment of additional nuclear-weapon-free zones by the time of the Review Conference in the year 2000 would be welcome.

7. The cooperation of all the nuclear-weapon States and their respect and support for the relevant protocols is necessary for the maximum effectiveness of such nuclear-weapon-free zones and the relevant protocols.

#### Security assurances

8. Noting United Nations Security Council resolution 984 (1995), which was adopted unanimously on 11 April 1995, as well as the declarations by the nuclear-weapon States concerning both negative and positive security assurances, further steps should be considered to assure non-nuclear-weapon States party to the Treaty against the use or threat of use of nuclear weapons. These steps could take the form of an internationally legally binding instrument.

#### Safeguards

9. The International Atomic Energy Agency (IAEA) is the competent authority responsible to verify and assure, in accordance with the statute of the IAEA and the Agency's safeguards system, compliance with its safeguards agreements with

States parties undertaken in fulfillment of their obligations under article III (1) of the Treaty, with a view to preventing diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices. Nothing should be done to undermine the authority of the IAEA in this regard. States parties that have concerns regarding non-compliance with the safeguards agreements of the Treaty by the States parties should direct such concerns, along with supporting evidence and information, to the IAEA to consider, investigate, draw conclusions and decide on necessary actions in accordance with its mandate.

10. All States parties required by article III of the Treaty to sign and bring into force comprehensive safeguards agreements and which have not yet done so should do so without delay.

11. IAEA safeguards should be regularly assessed and evaluated. Decisions adopted by its Board of Governors aimed at further strengthening the effectiveness of IAEA safeguards should be supported and implemented and the IAEA's capability to detect undeclared nuclear activities should be increased. Also States not party to the Treaty on the Non-Proliferation of Nuclear Weapons should be urged to enter into comprehensive safeguards agreements with the IAEA.

12. New supply arrangements for the transfer of source or special fissionable material or equipment or material especially designed or prepared for the processing, use or production of special fissionable material to non-nuclear-weapon States should require, as a necessary precondition, acceptance of IAEA full-scope safeguards and internationally legally binding commitments not to acquire nuclear weapons or other nuclear explosive devices.

13. Nuclear fissile material transferred from military use to peaceful nuclear activities should, as soon as practicable, be placed under IAEA safeguards in the framework of the voluntary safeguards agreements in place with the nuclear-weapon States. Safeguards should be universally applied once the complete elimination of nuclear weapons has been achieved.

#### Peaceful uses of nuclear energy

14. Particular importance should be attached to ensuring the exercise of the inalienable right of all the parties to the Treaty to develop research, production and use of nuclear energy for peaceful purposes without discrimination and in conformity with articles I, II as well as III of the Treaty.

15. Undertakings to facilitate participation in the fullest possible exchange of equipment, materials and scientific and technological information for the peaceful uses of nuclear energy should be fully implemented.

16. In all activities designed to promote the peaceful uses of nuclear energy, preferential treatment should be given to the non-nuclear-weapon States party to the Treaty, taking the needs of developing countries particularly into account.

17. Transparency in nuclear-related export controls should be promoted within the framework of dialogue and cooperation among all interested States party to the Treaty.

18. All States should, through rigorous national measures and international cooperation, maintain the highest practicable levels of nuclear safety, including in waste management, and observe standards and guidelines in nuclear materials accounting, physical protection and transport of nuclear materials.

19. Every effort should be made to ensure that the IAEA has the financial and human resources necessary in order to meet effectively its responsibilities in the areas of technical cooperation, safeguards and nuclear safety. The IAEA should also be encouraged to intensify its efforts aimed at finding ways and means for funding technical assistance through predictable and assured resources.

20. Attacks or threats of attack on nuclear facilities devoted to peaceful purposes jeopardize nuclear safety and raise serious concerns regarding the application of international law on the use of force in such cases, which could warrant appropriate action in accordance with the provisions of the Charter of the United Nations.

The Conference requests that the President of the Conference bring this decision, the Decision on Strengthening the Review Process for the Treaty and the Decision on the Extension of the Treaty to the attention of the heads of State or Government of all States and seek their full cooperation on these documents and in the furtherance of the goals of the Treaty.