Homeland Security Presidential Directive

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-1

October 29, 2001

Subject: Organization and Operation of the Homeland Security Council

This is the first in a series of Homeland Security Presidential Directives that shall record and communicate presidential decisions about the homeland security policies of the United States.

A. Homeland Security Council

Securing Americans from terrorist threats or attacks is a critical national security function. It requires extensive coordination across a broad spectrum of Federal, State, and local agencies to reduce the potential for terrorist attacks and to mitigate damage should such an attack occur. The Homeland Security Council (HSC) shall ensure coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.

B. The Homeland Security Council Principals Committee

The HSC Principals Committee (HSC/PC) shall be the senior interagency forum under the HSC for homeland security issues. The HSC/PC is composed of the following members: the Secretary of the Treasury; the Secretary of Defense; the Attorney General; the Secretary of Health and Human Services; the Secretary of Transportation; the Director of the Office of Management and Budget; the Assistant to the President for Homeland Security (who serves as Chairman); the Assistant to the President and Chief of Staff; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation; the Director of the Federal Emergency Management Agency; and the Assistant to the President and Chief of Staff to the Vice President. The Assistant to the President for National Security Affairs shall be invited to attend all meetings of the HSC/PC. The following people shall be invited to HSC/PC meetings when issues pertaining to their responsibilities and expertise are discussed: the Secretary of State; the Secretary of the Interior; the Secretary of Agriculture; the Secretary of Commerce; the Secretary of Labor; the Secretary of Energy; the Secretary of Veterans Affairs; the Administrator of the Environmental Protection Agency; and the Deputy National Security Advisor for Combating Terrorism. The Counsel to the President shall be consulted regarding the agenda of HSC/PC meetings and shall attend any meeting when, in consultation with the Assistant to the President for Homeland Security, the Counsel deems it appropriate. The Deputy Director of the Office of Homeland Security shall serve as Executive Secretary of the HSC/PC. Other heads of departments and agencies and senior officials shall be invited, when appropriate.

The HSC/PC shall meet at the call of the Assistant to the President for Homeland Security, in consultation with the regular attendees of the HSC/PC. The Assistant to the President for Homeland Security shall determine the agenda, in consultation with the regular attendees, and shall ensure that all necessary papers are prepared. When global terrorism with domestic

implications is on the agenda of the HSC/PC, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall perform these tasks in concert.

C. Homeland Security Council Deputies Committee

The HSC Deputies Committee (HSC/DC) shall serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting homeland security. The HSC/DC can task and review the work of the HSC interagency groups discussed below. The HSC/DC shall help ensure that issues brought before the HSC/PC or the HSC have been properly analyzed and prepared for action. The HSC/DC shall have the following as its regular members: the Deputy Secretary of the Treasury; the Deputy Secretary of Defense; the Deputy Attorney General; the Deputy Secretary of Health and Human Services; the Deputy Secretary of Transportation; the Deputy Director of the Office of Homeland Security (who serves as Chairman); the Deputy Director of Central Intelligence; the Deputy Director of the Federal Bureau of Investigation; the Deputy Director of the Federal Emergency Management Agency; the Deputy Director of the Office of Management and Budget; and the Assistant to the President and Chief of Staff to the Vice President. The Assistant to the President and Deputy National Security Advisor shall be invited to attend all meetings of the HSC/DC. The following people shall be invited to attend when issues pertaining to their responsibilities and expertise are to be discussed: the Deputy Secretary of State; the Deputy Secretary of the Interior; the Deputy Secretary of Agriculture; the Deputy Secretary of Commerce; the Deputy Secretary of Labor; the Deputy Secretary of Energy; the Deputy Secretary of Veterans Affairs; the Deputy Administrator of the Environmental Protection Agency; the Deputy National Security Advisor for Combating Terrorism; and the Special Advisor to the President for Cyber-space Security. The Executive Secretary of the Office of Homeland Security shall serve as Executive Secretary of the HSC/DC. Other senior officials shall be invited, when appropriate.

The HSC/DC shall meet at the call of its Chairman. Any regular member of the HSC/DC may request a meeting of the HSC/DC for prompt crisis management. For all meetings, the Chairman shall determine the agenda, in consultation with the regular members, and shall ensure that necessary papers are prepared.

D. Homeland Security Council Policy Coordination Committees

HSC Policy Coordination Committees (HSC/PCCs) shall coordinate the development and implementation of homeland security policies by multiple departments and agencies throughout the Federal government, and shall coordinate those policies with State and local government. The HSC/PCCs shall be the main day-to-day fora for interagency coordination of homeland security policy. They shall provide policy analysis for consideration by the more senior committees of the HSC system and ensure timely responses to decisions made by the President. Each HSC/PCC shall include representatives from the executive departments, offices, and agencies represented in the HSC/DC.

Eleven HSC/PCCs are hereby established for the following functional areas, each to be chaired by the designated Senior Director from the Office of Homeland Security:

1. Detection, Surveillance, and Intelligence (by the Senior Director, Intelligence and Detection);

2. Plans, Training, Exercises, and Evaluation (by the Senior Director, Policy and Plans);

3. Law Enforcement and Investigation (by the Senior Director, Intelligence and Detection);

4. Weapons of Mass Destruction (WMD) Consequence Management (by the Senior Director, Response and Recovery);

5. Key Asset, Border, Territorial Waters, and Airspace Security (by the Senior Director, Protection and Prevention);

6. Domestic Transportation Security (by the Senior Director, Protection and Prevention);

7. Research and Development (by the Senior Director, Research and Development);

8. Medical and Public Health Preparedness (by the Senior Director, Protection and Prevention);

9. Domestic Threat Response and Incident Management (by the Senior Director, Response and Recovery);

10. Economic Consequences (by the Senior Director, Response and Recovery); and

11. Public Affairs (by the Senior Director, Communications).

Each HSC/PCC shall also have an Executive Secretary to be designated by the Assistant to the President for Homeland Security (from the staff of the HSC). The Executive Secretary of each HSC/PCC shall assist his or her Chair in scheduling the meetings of the HSC/PCC, determining the agenda, recording the actions taken and tasks assigned, and ensuring timely responses to the central policy-making committees of the HSC system. The Chairman of each HSC/PCC, in consultation with its Executive Secretary, may invite representatives of other executive departments and agencies to attend meetings of the HSC/PCC, when appropriate.

The Assistant to the President for Homeland Security, at the direction of the President and in consultation with the Vice President, the Attorney General, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Transportation, and the Director of the Federal Emergency Management Agency, may establish additional HSC/PCCs, as appropriate.

The Chairman of each HSC/PCC, with the agreement of its Executive Secretary, may establish subordinate working groups to assist the PCC in the performance of its duties.

The Vice President may attend any and all meetings of any entity established by or under this directive.

This directive shall be construed in a manner consistent with Executive Order 13228.

GEORGE W. BUSH

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-2

October 29, 2001

SUBJECT: Combating Terrorism Through Immigration Policies

A. National Policy

The United States has a long and valued tradition of welcoming immigrants and visitors. But the attacks of September 11, 2001, showed that some come to the United States to commit terrorist acts, to raise funds for illegal terrorist activities, or to provide other support for terrorist operations, here and abroad. It is the policy of the United States to work aggressively to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.

1. Foreign Terrorist Tracking Task Force

By November 1, 2001, the Attorney General shall create the Foreign Terrorist Tracking Task Force (Task Force), with assistance from the Secretary of State, the Director of Central Intelligence and other officers of the government, as appropriate. The Task Force shall ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: 1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and 2) locate, detain, prosecute, or deport any such aliens already present in the United States.

The Attorney General shall appoint a senior official as the full-time Director of the Task Force. The Director shall report to the Deputy Attorney General, serve as a Senior Advisor to the Assistant to the President for Homeland Security, and maintain direct liaison with the Commissioner of the Immigration and Naturalization Service (INS) on issues related to immigration and the foreign terrorist presence in the United States. The Director shall also consult with the Assistant Secretary of State for Consular Affairs on issues related to visa matters.

The Task Force shall be staffed by expert personnel from the Department of State, the INS, the Federal Bureau of Investiga-tion, the Secret Service, the Customs Service, the Intelligence Community, military support components, and other Federal agencies as appropriate to accomplish the Task Force's mission.

The Attorney General and the Director of Central Intelligence shall ensure, to the maximum extent permitted by law, that the Task Force has access to all available information necessary to perform its mission, and they shall request information from State and local governments, where appropriate.

With the concurrence of the Attorney General and the Director of Central Intelligence, foreign liaison officers from cooperating countries shall be invited to serve as liaisons to the Task Force, where appropriate, to expedite investigation and data sharing.

Other Federal entities, such as the Migrant Smuggling and Trafficking in Persons Coordination Center and the Foreign Leads Development Activity, shall provide the Task Force with any relevant information they possess concerning aliens suspected of engaging in or supporting terrorist activity.

2. Enhanced INS and Customs Enforcement Capability

The Attorney General and the Secretary of the Treasury, assisted by the Director of Central Intelligence, shall immediately develop and implement multi-year plans to enhance the investigative and intelligence analysis capabilities of the INS and the Customs Service. The goal of this enhancement is to increase significantly efforts to identify, locate, detain, prosecute or deport aliens associated with, suspected of being engaged in, or supporting terrorist activity within the United States.

The new multi-year plans should significantly increase the number of Customs and INS special agents assigned to Joint Terrorism Task Forces, as deemed appropriate by the Attorney General and the Secretary of the Treasury. These officers shall constitute new positions over and above the existing on-duty special agent forces of the two agencies.

3. Abuse of International Student Status

The United States benefits greatly from international students who study in our country. The United States Government shall continue to foster and support international students.

The Government shall implement measures to end the abuse of student visas and prohibit certain international students from receiving education and training in sensitive areas, including areas of study with direct application to the development and use of weapons of mass destruction. The Government shall also prohibit the education and training of foreign nationals who would use such training to harm the United States or its Allies.

The Secretary of State and the Attorney General, working in conjunction with the Secretary of Education, the Director of the Office of Science and Technology Policy, the Secretary of Defense, the Secretary of Energy, and any other departments or entities they deem necessary, shall develop a program to accomplish this goal. The program shall identify sensitive courses of study, and shall include measures whereby the Depart-ment of State, the Department of Justice, and United States academic institutions, working together, can identify problematic applicants for student visas and deny their applications. The program shall provide for tracking the status of a foreign student who receives a visa (to include the proposed major course of study, the status of the individual as a full-time student, the classes in which the student enrolls, and the source of the funds supporting the student's education).

The program shall develop guidelines that may include control mechanisms, such as limited duration student immigration status, and may implement strict criteria for renewing such student immigration status. The program shall include guidelines for exempting students from countries or groups of countries from this set of requirements.

In developing this new program of control, the Secretary of State, the Attorney General, and the Secretary of Education shall consult with the academic community and other interested parties. This new program shall be presented through the Homeland Security Council to the President within 60 days.

The INS, in consultation with the Department of Education, shall conduct periodic reviews of all institutions certified to receive nonimmigrant students and exchange visitor program students. These reviews shall include checks for compliance with record keeping and reporting requirements. Failure of institutions to comply may result in the termination of the institution's approval to receive such students.

4. North American Complementary Immigration Policies

The Secretary of State, in coordination with the Secretary of the Treasury and the Attorney General, shall promptly initiate negotiations with Canada and Mexico to assure maximum possible compatibility of immigration, customs, and visa policies. The goal of the negotiations shall be to provide all involved countries the highest possible level of assurance that only individuals seeking entry for legitimate purposes enter any of the countries, while at the same time minimizing border restrictions that hinder legitimate trans-border commerce.

As part of this effort, the Secretaries of State and the Treasury and the Attorney General shall seek to substantially increase sharing of immigration and customs information. They shall also seek to establish a shared immigration and customs control data-base with both countries. The Secretary of State, the Secretary of the Treasury, and the Attorney General shall explore existing mechanisms to accomplish this goal and, to the maximum extent possible, develop new methods to achieve optimal effectiveness and relative transparency. To the extent statutory provisions prevent such information sharing, the Attorney General and the Secretaries of State and the Treasury shall submit to the Director of the Office of Management and Budget proposed remedial legislation.

5. Use of Advanced Technologies for Data Sharing and Enforcement Efforts

The Director of the OSTP, in conjunction with the Attorney General and the Director of Central Intelligence, shall make recommendations about the use of advanced technology to help enforce United States immigration laws, to implement United States immigration programs, to facilitate the rapid identification of aliens who are suspected of engaging in or supporting terrorist activity, to deny them access to the United States, and to recommend ways in which existing government databases can be best utilized to maximize the ability of the government to detect, identify, locate, and apprehend potential terrorists in the United States. Databases from all appropriate Federal agencies, state and local govern-ments, and commercial databases should be included in this review. The utility of advanced data mining software should also be addressed. To the extent

that there may be legal barriers to such data sharing, the Director of the OSTP shall submit to the Director of the Office of Management and Budget proposed legislative remedies. The study also should make recommendations, propose timelines, and project budgetary requirements.

The Director of the OSTP shall make these recommendations to the President through the Homeland Security Council within 60 days.

6. Budgetary Support

The Office of Management and Budget shall work closely with the Attorney General, the Secretaries of State and of the Treasury, the Assistant to the President for Homeland Security, and all other appropriate agencies to review the budgetary support and identify changes in legislation necessary for the implementation of this directive and recommend appropriate support for a multi-year program to provide the United States a robust capability to prevent aliens who engage in or support terrorist activity from entering or remaining in the United States or the smuggling of implements of terrorism into the United States. The Director of the Office of Management and Budget shall make an interim report through the Homeland Security Council to the President on the recommended program within 30 days, and shall make a final report through the Homeland Security Council to the President on the recommended program within 60 days.

GEORGE W. BUSH

March 11, 2002

Homeland Security Presidential Directive-3

Purpose

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

Homeland Security Advisory System

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green;

Guarded = Blue;

Elevated = Yellow;

High = Orange;

Severe = Red.

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response. Department and agency heads are respon-sible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures. They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations' Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information. The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable, these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity.

Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?

2. To what degree is the threat information corroborated?

3. To what degree is the threat specific and/or imminent?

4. How grave are the potential consequences of the threat?

Threat Conditions and Associated Protective Measures

The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific Protective Measures:

1. Low Condition (Green). This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:

a) Refining and exercising as appropriate preplanned Protective Measures;

b) Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and

c) Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

2. Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

a) Checking communications with designated emergency response or command locations;

b) Reviewing and updating emergency response procedures; and

c) Providing the public with any information that would strengthen its ability to act appropriately.

3. Elevated Condition (Yellow). An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:

a) Increasing surveillance of critical locations;

b) Coordinating emergency plans as appropriate with nearby jurisdictions;

c) Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and

d) Implementing, as appropriate, contingency and emergency response plans.

4. High Condition (Orange). A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

a) Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;

b) Taking additional precautions at public events and possibly considering alternative venues or even cancellation;

c) Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and

d) Restricting threatened facility access to essential personnel only.

5. Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

a) Increasing or redirecting personnel to address critical emergency needs;

b) Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;

c) Monitoring, redirecting, or constraining transportation systems; and

d) Closing public and government facilities.

Comment and Review Periods

The Attorney General, in consultation and coordination with the Assistant to the President for Homeland Security, shall, for 45 days from the date of this directive, seek the views of government officials at all levels and of public interest groups and the private sector on the proposed Homeland Security Advisory System.

One hundred thirty-five days from the date of this directive the Attorney General, after consultation and coordination with the Assistant to the President for Homeland Security, and having considered the views received during the comment period, shall recommend to the President in writing proposed refinements to the Homeland Security Advisory System.

GEORGE W. BUSH

The classified version of NSPD-17, as reported by the Washington Times on January 31, 2003, included this controversial sentence:

> "The United States will continue to make clear that it reserves the right to respond with overwhelming force — including potentially nuclear weapons — to the use of [weapons of mass destruction] against the United States, our forces abroad, and friends and allies."

NSPD-17 / HSPD 4 [unclassified version]:

National Strategy to Combat Weapons of Mass Destruction

December 2002

"The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed. ... History will judge harshly those who saw this coming danger but failed to act. In the new world we have entered, the only path to peace and security is the path of action."

President Bush
The National Security Strategy of the United States of America
September 17, 2002

INTRODUCTION

Weapons of mass destruction (WMD) -- nuclear, biological, and chemical -- in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States. We must pursue a comprehensive strategy to counter this threat in all of its dimensions.

An effective strategy for countering WMD, including their use and further proliferation, is an integral component of the National Security Strategy of the United States of America. As with the war on terrorism, our strategy for homeland security, and our new concept of deterrence, the U.S. approach to combat WMD represents a fundamental change from the past. To succeed, we must take full advantage of today's opportunities, including the application of new technologies, increased emphasis on intelligence collection and analysis, the strengthening of alliance relationships, and the establishment of new partnerships with former adversaries.

Weapons of mass destruction could enable adversaries to inflict massive harm on the United States, our military forces at home and abroad, and our friends and allies. Some states, including several that have supported and continue to support terrorism, already possess WMD and are seeking even greater capabilities, as tools of coercion and intimidation. For them, these are not weapons of last resort, but militarily useful weapons of choice intended to overcome our nation's advantages in conventional forces and to deter us from responding to aggression against our friends and allies in regions of vital interest. In addition, terrorist groups are seeking to acquire

WMD with the stated purpose of killing large numbers of our people and those of friends and allies -- without compunction and without warning.

We will not permit the world's most dangerous regimes and terrorists to threaten us with the world's most destructive weapons. We must accord the highest priority to the protection of the United States, our forces, and our friends and allies from the existing and growing WMD threat.

PILLARS OF OUR NATIONAL STRATEGY

Our National Strategy to Combat Weapons of Mass Destruction has three principal pillars:

Counterproliferation to Combat WMD Use

The possession and increased likelihood of use of WMD by hostile states and terrorists are realities of the contemporary security environment. It is therefore critical that the U. S. military and appropriate civilian agencies be prepared to deter and defend against the full range of possible WMD employment scenarios. We will ensure that all needed capabilities to combat WMD are fully integrated into the emerging defense transformation plan and into our homeland security posture. Counterproliferation will also be fully integrated into the basic doctrine, training, and equipping of all forces, in order to ensure that they can sustain operations to decisively defeat WMD-armed adversaries.

Strengthened Nonproliferation to Combat WMD Proliferation

The United States, our friends and allies, and the broader international community must undertake every effort to prevent states and terrorists from acquiring WMD and missiles. We must enhance traditional measures -- diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls -- that seek to dissuade or impede proliferant states and terrorist networks, as well as to slow and make more costly their access to sensitive technologies, material, and expertise. We must ensure compliance with relevant international agreements, including the Nuclear Nonproliferation Treaty (NPT), the Chemical Weapons Convention (CWC), and the Biological Weapons Convention (BWC). The United States will continue to work with other states to improve their capability to prevent unauthorized transfers of WMD and missile technology, expertise, and material. We will identify and pursue new methods of prevention, such as national criminalization of proliferation activities and expanded safety and security measures.

Consequence Management to Respond to WMD Use

Finally, the United States must be prepared to respond to the use of WMD against our citizens, our military forces, and those of friends and allies. We will develop and maintain the capability to reduce to the extent possible the potentially horrific consequences of WMD attacks at home and abroad.

The three pillars of the U.S. national strategy to combat WMD are seamless elements of a comprehensive approach. Serving to integrate the pillars are four cross-cutting enabling

functions that need to be pursued on a priority basis: intelligence collection and analysis on WMD, delivery systems, and related technologies; research and development to improve our ability to respond to evolving threats; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists.

COUNTERPROLIFERATION

We know from experience that we cannot always be successful in preventing and containing the proliferation of WMD to hostile states and terrorists. Therefore, U.S. military and appropriate civilian agencies must possess the full range of operational capabilities to counter the threat and use of WMD by states and terrorists against the United States, our military forces, and friends and allies.

Interdiction

Effective interdiction is a critical part of the U.S. strategy to combat WMD and their delivery means. We must enhance the capabilities of our military, intelligence, technical, and law enforcement communities to prevent the movement of WMD materials, technology, and expertise to hostile states and terrorist organizations.

Deterrence

Today's threats are far more diverse and less predictable than those of the past. States hostile to the United States and to our friends and allies have demonstrated their willingness to take high risks to achieve their goals, and are aggressively pursuing WMD and their means of delivery as critical tools in this effort. As a consequence, we require new methods of deterrence. A strong declaratory policy and effective military forces are essential elements of our contemporary deterrent posture, along with the full range of political tools to persuade potential adversaries not to seek or use WMD. The United States will continue to make clear that it reserves the right to respond with overwhelming force -- including through resort to all of our options -- to the use of WMD against the United States, our forces abroad, and friends and allies.

In addition to our conventional and nuclear response and defense capabilities, our overall deterrent posture against WMD threats is reinforced by effective intelligence, surveillance, interdiction, and domestic law enforcement capabilities. Such combined capabilities enhance deterrence both by devaluing an adversary's WMD and missiles, and by posing the prospect of an overwhelming response to any use of such weapons.

Defense and Mitigation

Because deterrence may not succeed, and because of the potentially devastating consequences of WMD use against our forces and civilian population, U.S. military forces and appropriate civilian agencies must have the capability to defend against WMD-armed adversaries, including in appropriate cases through preemptive measures. This requires capabilities to detect and destroy an adversary's WMD assets before these weapons are used. In addition, robust active and passive defenses and mitigation measures must be in place to enable U.S. military forces and

appropriate civilian agencies to accomplish their missions, and to assist friends and allies when WMD are used.

Active defenses disrupt, disable, or destroy WMD en route to their targets. Active defenses include vigorous air defense and effective missile defenses against today's threats. Passive defenses must be tailored to the unique characteristics of the various forms of WMD. The United States must also have the ability rapidly and effectively to mitigate the effects of a WMD attack against our deployed forces.

Our approach to defend against biological threats has long been based on our approach to chemical threats, despite the fundamental differences between these weapons. The United States is developing a new approach to provide us and our friends and allies with an effective defense against biological weapons.

Finally, U.S. military forces and domestic law enforcement agencies as appropriate must stand ready to respond against the source of any WMD attack. The primary objective of a response is to disrupt an imminent attack or an attack in progress, and eliminate the threat of future attacks. As with deterrence and prevention, an effective response requires rapid attribution and robust strike capability. We must accelerate efforts to field new capabilities to defeat WMD-related assets. The United States needs to be prepared to conduct post-conflict operations to destroy or dismantle any residual WMD capabilities of the hostile state or terrorist network. An effective U.S. response not only will eliminate the source of a WMD attack but will also have a powerful deterrent effect upon other adversaries that possess or seek WMD or missiles.

NONPROLIFERATION

Active Nonproliferation Diplomacy

The United States will actively employ diplomatic approaches in bilateral and multilateral settings in pursuit of our nonproliferation goals. We must dissuade supplier states from cooperating with proliferant states and induce proliferant states to end their WMD and missile programs. We will hold countries responsible for complying with their commitments. In addition, we will continue to build coalitions to support our efforts, as well as to seek their increased support for nonproliferation and threat reduction cooperation programs. However, should our wide-ranging nonproliferation efforts fail, we must have available the full range of operational capabilities necessary to defend against the possible employment of WMD.

Multilateral Regimes

Existing nonproliferation and arms control regimes play an important role in our overall strategy. The United States will support those regimes that are currently in force, and work to improve the effectiveness of, and compliance with, those regimes. Consistent with other policy priorities, we will also promote new agreements and arrangements that serve our nonproliferation goals. Overall, we seek to cultivate an international environment that is more conducive to nonproliferation. Our efforts will include:

- Nuclear
    - Strengthening of the Nuclear Nonproliferation Treaty and International Atomic Energy Agency (IAEA), including through ratification of an IAEA Additional Protocol by all NPT states parties, assurances that all states put in place full-scope IAEA safeguards agreements, and appropriate increases in funding for the Agency;
    - Negotiating a Fissile Material Cut-Off Treaty that advances U.S. security interests; and
    - Strengthening the Nuclear Suppliers Group and Zangger Committee.
- Chemical and Biological
    - Effective functioning of the Organization for the Prohibition of Chemical Weapons;
    - Identification and promotion of constructive and realistic measures to strengthen the BWC and thereby to help meet the biological weapons threat; and
    - Strengthening of the Australia Group.
- Missile
    - Strengthening the Missile Technology Control Regime (MTCR), including through support for universal adherence to the International Code of Conduct Against Ballistic Missile Proliferation.

Nonproliferation and Threat Reduction Cooperation

The United States pursues a wide range of programs, including the Nunn-Lugar program, designed to address the proliferation threat stemming from the large quantities of Soviet-legacy WMD and missile-related expertise and materials. Maintaining an extensive and efficient set of nonproliferation and threat reduction assistance programs to Russia and other former Soviet states is a high priority. We will also continue to encourage friends and allies to increase their contributions to these programs, particularly through the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. In addition, we will work with other states to improve the security of their WMD-related materials.

Controls on Nuclear Materials

In addition to programs with former Soviet states to reduce fissile material and improve the security of that which remains, the United States will continue to discourage the worldwide accumulation of separated plutonium and to minimize the use of highly-enriched uranium. As outlined in the National Energy Policy, the United States will work in collaboration with international partners to develop recycle and fuel treatment technologies that are cleaner, more efficient, less waste-intensive, and more proliferation-resistant.

U.S. Export Controls

We must ensure that the implementation of U.S. export controls furthers our nonproliferation and other national security goals, while recognizing the realities that American businesses face in the increasingly globalized marketplace.

We will work to update and strengthen export controls using existing authorities. We also seek new legislation to improve the ability of our export control system to give full weight to both nonproliferation objectives and commercial interests. Our overall goal is to focus our resources on truly sensitive exports to hostile states or those that engage in onward proliferation, while removing unnecessary barriers in the global marketplace.

Nonproliferation Sanctions

Sanctions can be a valuable component of our overall strategy against WMD proliferation. At times, however, sanctions have proven inflexible and ineffective. We will develop a comprehensive sanctions policy to better integrate sanctions into our overall strategy and work with Congress to consolidate and modify existing sanctions legislation.

WMD CONSEQUENCE MANAGEMENT

Defending the American homeland is the most basic responsibility of our government. As part of our defense, the United States must be fully prepared to respond to the consequences of WMD use on our soil, whether by hostile states or by terrorists. We must also be prepared to respond to the effects of WMD use against our forces deployed abroad, and to assist friends and allies.

The National Strategy for Homeland Security discusses U.S. Government programs to deal with the consequences of the use of a chemical, biological, radiological, or nuclear weapon in the United States. A number of these programs offer training, planning, and assistance to state and local governments. To maximize their effectiveness, these efforts need to be integrated and comprehensive. Our first responders must have the full range of protective, medical, and remediation tools to identify, assess, and respond rapidly to a WMD event on our territory.

The White House Office of Homeland Security will coordinate all federal efforts to prepare for and mitigate the consequences of terrorist attacks within the United States, including those involving WMD. The Office of Homeland Security will also work closely with state and local governments to ensure their planning, training, and equipment requirements are addressed. These issues, including the roles of the Department of Homeland Security, are addressed in detail in the National Strategy for Homeland Security.

The National Security Council's Office of Combating Terrorism coordinates and helps improve U. S. efforts to respond to and manage the recovery from terrorist attacks outside the United States. In cooperation with the Office of Combating Terrorism, the Department of State coordinates interagency efforts to work with our friends and allies to develop their own emergency preparedness and consequence management capabilities.

INTEGRATING THE PILLARS

Several critical enabling functions serve to integrate the three pillars -- counterproliferation, nonproliferation, and consequence management -- of the U.S. National Strategy to Combat WMD.

Improved Intelligence Collection and Analysis

A more accurate and complete understanding of the full range of WMD threats is, and will remain, among the highest U. S. intelligence priorities, to enable us to prevent proliferation, and to deter or defend against those who would use those capabilities against us. Improving our ability to obtain timely and accurate knowledge of adversaries' offensive and defensive capabilities, plans, and intentions is key to developing effective counter-and nonproliferation policies and capabilities. Particular emphasis must be accorded to improving: intelligence regarding WMD-related facilities and activities; interaction among U.S. intelligence, law enforcement, and military agencies; and intelligence cooperation with friends and allies.

Research and Development

The United States has a critical need for cutting-edge technology that can quickly and effectively detect, analyze, facilitate interdiction of, defend against, defeat, and mitigate the consequences of WMD. Numerous U.S. Government departments and agencies are currently engaged in the essential research and development to support our overall strategy against WMD proliferation.

The new Counterproliferation Technology Coordination Committee, consisting of senior representatives from all concerned agencies, will act to improve interagency coordination of U.S. Government counterproliferation research and development efforts. The Committee will assist in identifying priorities, gaps, and overlaps in existing programs and in examining options for future investment strategies.

Strengthened International Cooperation

WMD represent a threat not just to the United States, but also to our friends and allies and the broader international community. For this reason, it is vital that we work closely with like-minded countries on all elements of our comprehensive proliferation strategy.

Targeted Strategies Against Proliferants

All elements of the overall U. S. strategy to combat WMD must be brought to bear in targeted strategies against supplier and recipient states of WMD proliferation concern, as well as against terrorist groups which seek to acquire WMD.

A few states are dedicated proliferators, whose leaders are determined to develop, maintain, and improve their WMD and delivery capabilities, which directly threaten the United States, U.S. forces overseas, and/or our friends and allies. Because each of these regimes is different, we will pursue country-specific strategies that best enable us and our friends and allies to prevent, deter, and defend against WMD and missile threats from each of them. These strategies must also take

into account the growing cooperation among proliferant states -- so-called secondary proliferation -- which challenges us to think in new ways about specific country strategies.

One of the most difficult challenges we face is to prevent, deter, and defend against the acquisition and use of WMD by terrorist groups. The current and potential future linkages between terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. The full range of counterproliferation, nonproliferation, and consequence management measures must be brought to bear against the WMD terrorist threat, just as they are against states of greatest proliferation concern.

END NOTE

Our National Strategy to Combat WMD requires much of all of us -- the Executive Branch, the Congress, state and local governments, the American people, and our friends and allies. The requirements to prevent, deter, defend against, and respond to today's WMD threats are complex and challenging. But they are not daunting. We can and will succeed in the tasks laid out in this strategy; we have no other choice.

Homeland Security Presidential Directive/HSPD-5

Subject: Management of Domestic Incidents

Purpose

(1) To enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.

Definitions

(2) In this directive:

(a) the term "Secretary" means the Secretary of Homeland Security.

(b) the term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, together with the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(c) the terms "State," "local," and the "United States" when it is used in a geographical sense, have the same meanings as used in the Homeland Security Act of 2002, Public Law 107-296.

Policy

(3) To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions.

(4) The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters,

or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.

(5) Nothing in this directive alters, or impedes the ability to carry out, the authorities of Federal departments and agencies to perform their responsibilities under law. All Federal departments and agencies shall cooperate with the Secretary in the Secretary's domestic incident management role.

(6) The Federal Government recognizes the roles and responsibilities of State and local authorities in domestic incident management. Initial responsibility for managing domestic incidents generally falls on State and local authorities. The Federal Government will assist State and local authorities when their

resources are overwhelmed, or when Federal interests are involved. The Secretary will coordinate with State and local governments to ensure adequate planning, equipment, training, and exercise activities. The Secretary will also provide assistance to State and local governments to develop all-hazards plans and capabilities, including those of greatest importance to the security of the United States, and will ensure that State, local, and Federal plans are compatible.

(7) The Federal Government recognizes the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. The Secretary will coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities.

(8) The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with United States law and with activities of other Federal departments and agencies to protect our national security, to assisting the Attorney General to identify the perpetrators and bring them to justice. The Attorney General and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(9) Nothing in this directive impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures. The Secretary of Defense shall provide military support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law. The Secretary of Defense shall retain command of military forces providing civil support. The Secretary of Defense and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(10) The Secretary of State has the responsibility, consistent with other United States Government activities to protect our national security, to coordinate international activities related to the prevention, preparation, response, and recovery from a domestic incident, and for the protection of United States citizens and United States interests overseas. The Secretary of State and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments.

(11) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall be responsible for interagency policy coordination on domestic and international incident management, respectively, as directed by the President. The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall work together to ensure that the United States domestic and international incident management efforts are seamlessly united.

(12) The Secretary shall ensure that, as appropriate, information related to domestic incidents is gathered and provided to the public, the private sector, State and local authorities, Federal departments and agencies, and, generally through the Assistant to the President for Homeland Security, to the President.

The Secretary shall provide standardized, quantitative reports to the Assistant to the President for Homeland Security on the readiness and preparedness of the Nation -- at all levels of government -- to prevent, prepare for, respond to, and recover from domestic incidents.

(13) Nothing in this directive shall be construed to grant to any Assistant to the President any authority to issue orders to Federal departments and agencies, their officers, or their employees.

Tasking

(14) The heads of all Federal departments and agencies are directed to provide their full and prompt cooperation, resources, and support, as appropriate and consistent with their own responsibilities for protecting our national security, to the Secretary, the Attorney General, the Secretary of Defense, and the Secretary of State in the exercise of the individual leadership responsibilities and missions assigned in paragraphs (4), (8), (9), and (10), respectively, above.

(15) The Secretary shall develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.

(16) The Secretary shall develop, submit for review to the Homeland Security Council, and administer a National Response Plan (NRP). The Secretary shall consult with appropriate Assistants to the President (including the Assistant to the President for Economic Policy) and the Director of the Office of Science and Technology Policy, and other such Federal officials as may be appropriate, in developing and implementing the NRP. This plan shall integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan. The NRP shall be unclassified. If certain operational aspects require classification, they shall be included in classified annexes to the NRP.

(a) The NRP, using the NIMS, shall, with regard to response to domestic incidents, provide the structure and mechanisms for national level policy and operational direction for Federal support to State and local incident managers and for exercising direct Federal authorities and responsibilities, as appropriate.

(b) The NRP will include protocols for operating under different threats or threat levels; incorporation of existing Federal emergency and incident management plans (with appropriate modifications and revisions) as either integrated components of the NRP or as supporting operational plans; and additional opera-tional plans or annexes, as appropriate, including public affairs and intergovernmental communications.

(c) The NRP will include a consistent approach to reporting incidents, providing assessments, and making recommendations to the President, the Secretary, and the Homeland Security Council.

(d) The NRP will include rigorous requirements for continuous improvements from testing, exercising, experience with incidents, and new information and technologies.

(17) The Secretary shall:

(a) By April 1, 2003, (1) develop and publish an initial version of the NRP, in consultation with other Federal departments and agencies; and (2) provide the Assistant to the President for Homeland Security with a plan for full development and implementation of the NRP.

(b) By June 1, 2003, (1) in consultation with Federal departments and agencies and with State and local governments, develop a national system of standards, guidelines, and protocols to implement the NIMS; and (2) establish a mechanism for ensuring ongoing management and maintenance of the NIMS, including regular consultation with other Federal departments and agencies and with State and local governments.

(c) By September 1, 2003, in consultation with Federal departments and agencies and the Assistant to the President for Homeland Security, review existing authorities and regulations and prepare recommendations for the President on revisions necessary to implement fully the NRP.

(18) The heads of Federal departments and agencies shall adopt the NIMS within their departments and agencies and shall provide support and assistance to the Secretary in the development and maintenance of the NIMS. All Federal departments and agencies will use the NIMS in their domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation activities, as well as those actions taken in support of State or local entities. The heads of Federal departments and agencies shall participate in the NRP, shall assist and support the Secretary in the development and maintenance of the NRP, and shall participate in and use domestic incident reporting systems and protocols established by the Secretary.

(19) The head of each Federal department and agency shall:

(a) By June 1, 2003, make initial revisions to existing plans in accordance with the initial version of the NRP.

(b) By August 1, 2003, submit a plan to adopt and implement the NIMS to the Secretary and the Assistant to the President for Homeland Security. The Assistant to the President for Homeland Security shall advise the President on whether such plans effectively implement the NIMS.

(20) Beginning in Fiscal Year 2005, Federal departments and agencies shall make adoption of the NIMS a requirement, to the extent permitted by law, for providing Federal preparedness assistance through grants, contracts, or other activities. The Secretary shall develop standards and guidelines for determining whether a State or local entity has adopted the NIMS.

Technical and Conforming Amendments to National Security Presidential Directive-1 (NSPD-1)

(21) NSPD-1 ("Organization of the National Security Council System") is amended by replacing the fifth sentence of the third paragraph on the first page with the following: "The Attorney General, the Secretary of Homeland Security, and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities.".

Technical and Conforming Amendments to National Security Presidential Directive-8 (NSPD-8)

(22) NSPD-8 ("National Director and Deputy National Security Advisor for Combating Terrorism") is amended by striking "and the Office of Homeland Security," on page 4, and inserting "the Department of Homeland Security, and the Homeland Security Council" in lieu thereof.

Technical and Conforming Amendments to Homeland Security Presidential Directive-2 (HSPD-2)

(23) HSPD-2 ("Combating Terrorism Through Immigration Policies") is amended as follows:

(a) striking "the Commissioner of the Immigration and Naturalization Service (INS)" in the second sentence of the second paragraph in section 1, and inserting "the Secretary of Homeland Security" in lieu thereof ;

(b) striking "the INS," in the third paragraph in section 1, and inserting "the Department of Homeland Security" in lieu thereof;

(c) inserting ", the Secretary of Homeland Security," after "The Attorney General" in the fourth paragraph in section 1;

(d) inserting ", the Secretary of Homeland Security," after "the Attorney General" in the fifth paragraph in section 1;

(e) striking "the INS and the Customs Service" in the first sentence of the first paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;

(f) striking "Customs and INS" in the first sentence of the second paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;

(g) striking "the two agencies" in the second sentence of the second paragraph of section 2, and inserting "the Department of Homeland Security" in lieu thereof;

(h) striking "the Secretary of the Treasury" wherever it appears in section 2, and inserting "the Secretary of Homeland Security" in lieu thereof;

(i) inserting ", the Secretary of Homeland Security," after "The Secretary of State" wherever the latter appears in section 3;

(j) inserting ", the Department of Homeland Security," after "the Department of State," in the second sentence in the third paragraph in section 3;

(k) inserting "the Secretary of Homeland Security," after "the Secretary of State," in the first sentence of the fifth paragraph of section 3;

(l) striking "INS" in the first sentence of the sixth paragraph of section 3, and inserting "Department of Homeland Security" in lieu thereof;

(m) striking "the Treasury" wherever it appears in section 4 and inserting "Homeland Security" in lieu thereof;

(n) inserting ", the Secretary of Homeland Security," after "the Attorney General" in the first sentence in section 5; and

(o) inserting ", Homeland Security" after "State" in the first sentence of section 6.

Technical and Conforming Amendments to Homeland Security Presidential Directive-3 (HSPD-3)

(24) The Homeland Security Act of 2002 assigned the responsibility for administering the Homeland Security Advisory System to the Secretary of Homeland Security. Accordingly, HSPD-3 of March 11, 2002 ("Homeland Security Advisory System") is amended as follows:

(a) replacing the third sentence of the second paragraph entitled "Homeland Security Advisory System" with "Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned."

(b) inserting "At the request of the Secretary of Homeland Security, the Department of Justice shall permit and facilitate the use of delivery systems administered or managed by the Department of Justice for the purposes of delivering threat information pursuant to the Homeland Security Advisory System." as a new paragraph after the fifth paragraph of the section entitled "Homeland Security Advisory System."

(c) inserting ", the Secretary of Homeland Security" after "The Director of Central Intelligence" in the first sentence of the seventh paragraph of the section entitled "Homeland Security Advisory System".

(d) striking "Attorney General" wherever it appears (except in the sentences referred to in subsections (a) and (c) above), and inserting "the Secretary of Homeland Security" in lieu thereof; and

(e) striking the section entitled "Comment and Review Periods."

GEORGE W. BUSH

Homeland Security Presidential Directive/Hspd-6

Subject: Integration and Use of Screening Information

To protect against terrorism it is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

This directive shall be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans.

To further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism, and to the full extent permitted by law and consistent with the policy set forth above:

(1) The Attorney General shall establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes.

(2) The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.

(3) The heads of executive departments and agencies shall conduct screening using such information at all appropriate opportunities, and shall report to the Attorney General not later than 90 days from the date of this directive, as to the opportunities at which such screening shall and shall not be conducted.

(4) The Secretary of Homeland Security shall develop guidelines to govern the use of such information to support State, local, territorial, and tribal screening processes, and private sector screening processes that have a substantial bearing on homeland security.

(5) The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.

This directive does not alter existing authorities or responsibilities of department and agency heads to carry out operational activities or provide or receive information. This directive is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

The Attorney General, in consultation with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence, shall report to me through the Assistant to the President for

Homeland Security not later than October 31, 2003, on progress made to implement this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

Homeland Security Presidential Directive / HSPD-7

Subject: Critical Infrastructure Identification, Prioritization, and Protection

Purpose

(1) This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Background

(2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Definitions

(6) In this directive:

> (a) The term "critical infrastructure" has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).
>
> (b) The term "key resources" has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term "the Department" means the Department of Homeland Security.

(d) The term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(e) The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(f) The term "the Secretary" means the Secretary of Homeland Security.

(g) The term "Sector-Specific Agency" means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities under this directive in accordance with guidance provided by the Secretary.

(h) The terms "protect" and "secure" mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Policy

(7) It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

(a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

(c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

(d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

(e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

(f) undermine the public's morale and confidence in our national economic and political institutions.

(8) Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.

(9) Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

(10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

(11) Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

Roles and Responsibilities of the Secretary

(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

(13) Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.

(14) The Secretary will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(15) The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities. In addition, in its role as overall cross-sector coordinator, the Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(16) The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector,

academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

(17) The Secretary will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.

Roles and Responsibilities of Sector-Specific Federal Agencies

(18) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:

(a) Department of Agriculture -- agriculture, food (meat, poultry, egg products);

(b) Health and Human Services -- public health, healthcare, and food (other than meat, poultry, egg products);

(c) Environmental Protection Agency -- drinking water and water treatment systems;

(d) Department of Energy -- energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;

(e) Department of the Treasury -- banking and finance;

(f) Department of the Interior -- national monuments and icons; and

(g) Department of Defense -- defense industrial base.

(19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:

(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;

(b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

(20) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Roles and Responsibilities of Other Departments, Agencies, and Offices

(22) In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.

(a) The Department of State, in conjunction with the Department, and the Departments of Justice, Commerce, Defense, the Treasury and other appropriate agencies, will work with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources.

(b) The Department of Justice, including the Federal Bureau of Investigation, will reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources. The Attorney General and the Secretary shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by presidential directive.

(c) The Department of Commerce, in coordination with the Department, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

(d) A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. This PCC will be chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.

(e) The Office of Science and Technology Policy, in coordination with the Department, will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources.

(f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident

center consistent with the requirements of the Federal Information Security Management Act of 2002.

(g) Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.

(h) The Department of Transportation and the Department will collaborate on all matters relating to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. The Department of Transportation and the Department will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines).

(i) All Federal departments and agencies shall work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

(23) The heads of all Federal departments and agencies will coordinate and cooperate with the Secretary as appropriate and consistent with their own responsibilities for protecting critical infrastructure and key resources.

(24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Coordination with the Private Sector

(25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

National Special Security Events

(26) The Secretary, after consultation with the Homeland Security Council, shall be responsible for designating events as "National Special Security Events" (NSSEs). This directive supersedes language in previous presidential directives regarding the designation of NSSEs that is inconsistent herewith.

Implementation

(27) Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, in addition to other Homeland Security-related elements as the Secretary deems appropriate, the following elements:

> (a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;
>
> (b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;
>
> (c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and
>
> (d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.

(28) The Secretary, consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

(29) The Secretary will continue to work with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy in order to ensure the necessary protection of:

> (a) commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training;
>
> (b) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and
>
> (c) the transportation, storage, and disposal of nuclear materials and waste.

(30) In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare on an annual basis a Federal Research and Development Plan in support of this directive.

(31) The Secretary will collaborate with other appropriate Federal departments and agencies to develop a program, consistent with applicable law, to geospatially map, image, analyze, and sort critical infrastructure and key resources by utilizing commercial satellite and airborne systems, and existing capabilities within other agencies. National technical means should be considered as an option of last resort. The Secretary, with advice from the Director of Central Intelligence, the Secretaries of Defense and the Interior, and the heads of other appropriate Federal departments and agencies, shall develop mechanisms for accomplishing this initiative. The Attorney General shall provide legal advice as necessary.

(32) The Secretary will utilize existing, and develop new, capabilities as needed to model comprehensively the potential implications of terrorist exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate with the Secretary to develop appropriate mechanisms for accomplishing this initiative.

(33) The Secretary will develop a national indications and warnings architecture for infrastructure protection and capabilities that will facilitate:

(a) an understanding of baseline infrastructure operations;

(b) the identification of indicators and precursors to an attack; and

(c) a surge capacity for detecting and analyzing patterns of potential attacks.

In developing a national indications and warnings architecture, the Department will work with Federal, State, local, and non-governmental entities to develop an integrated view of physical and cyber infrastructure and key resources.

(34) By July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

(35) On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors. The report shall be submitted within 1 year from the issuance of this directive and on an annual basis thereafter.

(36) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs will lead a national security and emergency preparedness communications policy review, with the heads of the appropriate Federal departments and

agencies, related to convergence and next generation architecture. Within 6 months after the issuance of this directive, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall submit for my consideration any recommended changes to such policy.

(37) This directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of any inconsistency. Moreover, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall jointly submit for my consideration a Presidential directive to make changes in Presidential directives issued prior to this date that conform such directives to this directive.

(38) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH

Homeland Security Presidential Directive / HSPD-8

Subject: National Preparedness

Purpose

(1) This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

Definitions

(2) For the purposes of this directive:

(a) The term "all-hazards preparedness" refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies.

(b) The term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(c) The term "Federal preparedness assistance" means Federal department and agency grants, cooperative agreements, loans, loan guarantees, training, and/or technical assistance provided to State and local governments and the private sector to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Unless noted otherwise, the term "assistance" will refer to Federal assistance programs.

(d) The term "first responder" refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.

(e) The terms "major disaster" and "emergency" have the meanings given in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(f) The term "major events" refers to domestic terrorist attacks, major disasters, and other emergencies.

(g) The term "national homeland security preparedness-related exercises" refers to homeland security-related exercises that train and test national decision makers and utilize resources of multiple Federal departments and agencies. Such exercises may involve State and local first responders when appropriate. Such exercises do not include those exercises conducted solely within a single Federal department or agency.

(h) The term "preparedness" refers to the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events. The term "readiness" is used interchangeably with preparedness.

(i) The term "prevention" refers to activities undertaken by the first responder community during the early stages of an incident to reduce the likelihood or consequences of threatened or actual terrorist attacks. More general and broader efforts to deter, disrupt, or thwart terrorism are not addressed in this directive.

(j) The term "Secretary" means the Secretary of Homeland Security.

(k) The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

Relationship to HSPD-5

(3) This directive is a companion to HSPD-5, which identifies steps for improved coordination in response to incidents. This directive describes the way Federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident.

Development of a National Preparedness Goal

(4) The Secretary is the principal Federal official for coordinating the implementation of all-hazards preparedness in the United States. In cooperation with other Federal departments and agencies, the Secretary coordinates the preparedness of Federal response assets, and the support for, and assessment of, the preparedness of State and local first responders.

(5) To help ensure the preparedness of the Nation to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies, the Secretary, in coordination with the heads of other appropriate Federal departments and agencies and in consultation with State and local governments, shall develop a national domestic all-hazards preparedness goal. Federal departments and agencies will work to achieve this goal by:

(a) providing for effective, efficient, and timely delivery of Federal preparedness assistance to State and local governments; and

(b) supporting efforts to ensure first responders are prepared to respond to major events, especially prevention of and response to threatened terrorist attacks.

(6) The national preparedness goal will establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them. It will also include readiness metrics and elements that support the national preparedness goal including standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism.

(7) The Secretary will submit the national preparedness goal to me through the Homeland Security Council (HSC) for review and approval prior to, or concurrently with, the Department of Homeland Security's Fiscal Year 2006 budget submission to the Office of Management and Budget.

Federal Preparedness Assistance

(8) The Secretary, in coordination with the Attorney General, the Secretary of Health and Human Services (HHS), and the heads of other Federal departments and agencies that provide assistance for first responder preparedness, will establish a single point of access to Federal preparedness assistance program information within 60 days of the issuance of this directive. The Secretary will submit to me through the HSC recommendations of specific Federal department and agency programs to be part of the coordinated approach. All Federal departments and agencies will cooperate with this effort. Agencies will continue to issue financial assistance awards consistent with applicable laws and regulations and will ensure that program announcements, solicitations, application instructions, and other guidance documents are consistent with other Federal preparedness programs to the extent possible. Full implementation of a closely coordinated interagency grant process will be completed by September 30, 2005.

(9) To the extent permitted by law, the primary mechanism for delivery of Federal preparedness assistance will be awards to the States. Awards will be delivered in a form that allows the recipients to apply the assistance to the highest priority preparedness requirements at the appropriate level of government. To the extent permitted by law, Federal preparedness assistance will be predicated on adoption of Statewide comprehensive all-hazards preparedness strategies. The strategies should be consistent with the national preparedness goal, should assess the most effective ways to enhance preparedness, should address areas facing higher risk, especially to terrorism, and should also address local government concerns and Citizen Corps efforts. The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, will review and approve strategies submitted by the States. To the extent permitted by law, adoption of approved Statewide strategies will be a requirement for receiving Federal preparedness assistance at all levels of government by September 30, 2005.

(10) In making allocations of Federal preparedness assistance to the States, the Secretary, the Attorney General, the Secretary of HHS, the Secretary of Transportation, the Secretary of Energy, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection

Agency, and the heads of other Federal departments and agencies that provide assistance for first responder preparedness will base those allocations on assessments of population concentrations, critical infrastructures, and other significant risk factors, particularly terrorism threats, to the extent permitted by law.

(11) Federal preparedness assistance will support State and local entities' efforts including planning, training, exercises, interoperability, and equipment acquisition for major events as well as capacity building for prevention activities such as information gathering, detection, deterrence, and collaboration related to terrorist attacks. Such assistance is not primarily intended to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism.

(12) The Attorney General, the Secretary of HHS, the Secretary of Transportation, the Secretary of Energy, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, and the heads of other Federal departments and agencies that provide assistance for first responder preparedness shall coordinate with the Secretary to ensure that such assistance supports and is consistent with the national preparedness goal.

(13) Federal departments and agencies will develop appropriate mechanisms to ensure rapid obligation and disbursement of funds from their programs to the States, from States to the local community level, and from local entities to the end users to derive maximum benefit from the assistance provided. Federal departments and agencies will report annually to the Secretary on the obligation, expenditure status, and the use of funds associated with Federal preparedness assistance programs.

Equipment

(14) The Secretary, in coordination with State and local officials, first responder organizations, the private sector and other Federal civilian departments and agencies, shall establish and implement streamlined procedures for the ongoing development and adoption of appropriate first responder equipment standards that support nationwide interoperability and other capabilities consistent with the national preparedness goal, including the safety and health of first responders.

(15) To the extent permitted by law, equipment purchased through Federal preparedness assistance for first responders shall conform to equipment standards in place at time of purchase. Other Federal departments and agencies that support the purchase of first responder equipment will coordinate their programs with the Department of Homeland Security and conform to the same standards.

(16) The Secretary, in coordination with other appropriate Federal departments and agencies and in consultation with State and local governments, will develop plans to identify and address national first responder equipment research and development needs based upon assessments of current and future threats. Other Federal departments and agencies that support preparedness research and development activities shall coordinate their efforts with the Department of Homeland Security and ensure they support the national preparedness goal.

Training and Exercises

(17) The Secretary, in coordination with the Secretary of HHS, the Attorney General, and other appropriate Federal departments and agencies and in consultation with State and local governments, shall establish and maintain a comprehensive training program to meet the national preparedness goal. The program will identify standards and maximize the effectiveness of existing Federal programs and financial assistance and include training for the Nation's first responders, officials, and others with major event preparedness, prevention, response, and recovery roles. Federal departments and agencies shall include private organizations in the accreditation and delivery of preparedness training as appropriate and to the extent permitted by law.

(18) The Secretary, in coordination with other appropriate Federal departments and agencies, shall establish a national program and a multi-year planning system to conduct homeland security preparedness-related exercises that reinforces identified training standards, provides for evaluation of readiness, and supports the national preparedness goal. The establishment and maintenance of the program will be conducted in maximum collaboration with State and local governments and appropriate private sector entities. All Federal departments and agencies that conduct national homeland security preparedness-related exercises shall participate in a collaborative, interagency process to designate such exercises on a consensus basis and create a master exercise calendar. The Secretary will ensure that exercises included in the calendar support the national preparedness goal. At the time of designation, Federal departments and agencies will identify their level of participation in national homeland security preparedness-related exercises. The Secretary will develop a multi-year national homeland security preparedness-related exercise plan and submit the plan to me through the HSC for review and approval.

(19) The Secretary shall develop and maintain a system to collect, analyze, and disseminate lessons learned, best practices, and information from exercises, training events, research, and other sources, including actual incidents, and establish procedures to improve national preparedness to prevent, respond to, and recover from major events. The Secretary, in coordination with other Federal departments and agencies and State and local governments, will identify relevant classes of homeland-security related information and appropriate means of transmission for the information to be included in the system. Federal departments and agencies are directed, and State and local governments are requested, to provide this information to the Secretary to the extent permitted by law.

Federal Department and Agency Preparedness

(20) The head of each Federal department or agency shall undertake actions to support the national preparedness goal, including adoption of quantifiable performance measurements in the areas of training, planning, equipment, and exercises for Federal incident management and asset preparedness, to the extent permitted by law. Specialized Federal assets such as teams, stockpiles, and caches shall be maintained at levels consistent with the national preparedness goal and be available for response activities as set forth in the National Response Plan, other appropriate operational documents, and applicable authorities or guidance. Relevant Federal

regulatory requirements should be consistent with the national preparedness goal. Nothing in this directive shall limit the authority of the Secretary of Defense with regard to the command and control, training, planning, equipment, exercises, or employment of Department of Defense forces, or the allocation of Department of Defense resources.

(21) The Secretary, in coordination with other appropriate Federal civilian departments and agencies, shall develop and maintain a Federal response capability inventory that includes the performance parameters of the capability, the timeframe within which the capability can be brought to bear on an incident, and the readiness of such capability to respond to domestic incidents. The Department of Defense will provide to the Secretary information describing the organizations and functions within the Department of Defense that may be utilized to provide support to civil authorities during a domestic crisis.

Citizen Participation

(22) The Secretary shall work with other appropriate Federal departments and agencies as well as State and local governments and the private sector to encourage active citizen participation and involvement in preparedness efforts. The Secretary shall periodically review and identify the best community practices for integrating private citizen capabilities into local preparedness efforts.

Public Communication

(23) The Secretary, in consultation with other Federal departments and agencies, State and local governments, and non-governmental organizations, shall develop a comprehensive plan to provide accurate and timely preparedness information to public citizens, first responders, units of government, the private sector, and other interested parties and mechanisms for coordination at all levels of government.

Assessment and Evaluation

(24) The Secretary shall provide to me through the Assistant to the President for Homeland Security an annual status report of the Nation's level of preparedness, including State capabilities, the readiness of Federal civil response assets, the utilization of mutual aid, and an assessment of how the Federal first responder preparedness assistance programs support the national preparedness goal. The first report will be provided within 1 year of establishment of the national preparedness goal.

(25) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(26) Actions pertaining to the funding and administration of financial assistance and all other activities, efforts, and policies in this directive shall be executed in accordance with law. To the extent permitted by law, these policies will be established and carried out in consultation with State and local governments.

(27) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH

February 3, 2004

Homeland Security Presidential Directive/HSPD-9

January 30, 2004

Subject: Defense of United States Agriculture and Food

Purpose

(1) This directive establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

Background

(2) The United States agriculture and food systems are vulnerable to disease, pest, or poisonous agents that occur naturally, are unintentionally introduced, or are intentionally delivered by acts of terrorism. Americas agriculture and food system is an extensive, open, interconnected, diverse, and complex structure providing potential targets for terrorist attacks. We should provide the best protection possible against a successful attack on the United States agriculture and food system, which could have catastrophic health and economic effects.

Definitions

(3) In this directive:

(a) The term critical infrastructure has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c (e)).

(b) The term key resources has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term Federal departments and agencies means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(d) The terms State, and local government, when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(e) The term Sector-Specific Agency means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

Policy

(4) It is the policy of the United States to protect the agriculture and food system from terrorist attacks, major disasters, and other emergencies by:

(a) identifying and prioritizing sector-critical infrastructure and key resources for establishing protection requirements;

(b) developing awareness and early warning capabilities to recognize threats;

(c) mitigating vulnerabilities at critical production and processing nodes;

(d) enhancing screening procedures for domestic and imported products; and

(e) enhancing response and recovery procedures.

(5) In implementing this directive, Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

Roles and Responsibilities

(6) As established in Homeland Security Presidential Directive-7 (HSPD-7), the Secretary of Homeland Security is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary of Homeland Security shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources. This directive shall be implemented in a manner consistent with HSPD-7.

(7) The Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency will perform their responsibilities as Sector-Specific Agencies as delineated in HSPD-7.

Awareness and Warning

(8) The Secretaries of the Interior, Agriculture, Health and Human Services, the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies shall build upon and expand current monitoring and surveillance programs to:

(a) develop robust, comprehensive, and fully coordinated surveillance and monitoring systems, including international information, for animal disease, plant disease, wildlife disease, food, public health, and water quality that provides early detection and awareness of disease, pest, or poisonous agents;

(b) develop systems that, as appropriate, track specific animals and plants, as well as specific commodities and food; and

(c) develop nationwide laboratory networks for food, veterinary, plant health, and water quality that integrate existing Federal and State laboratory resources, are interconnected, and utilize standardized diagnostic protocols and procedures.

(9) The Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, in coordination with the Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency, shall develop and enhance intelligence operations and analysis capabilities focusing on the agriculture, food, and water sectors. These intelligence capabilities will include collection and analysis of information concerning threats, delivery systems, and methods that could be directed against these sectors.

(10) The Secretary of Homeland Security shall coordinate with the Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies to create a new biological threat awareness capacity that will enhance detection and characterization of an attack. This new capacity will build upon the

improved and upgraded surveillance systems described in paragraph 8 and integrate and analyze domestic and international surveillance and monitoring data collected from human health, animal health, plant health, food, and water quality systems. The Secretary of Homeland Security will submit a report to me through the Homeland Security Council within 90 days of the date of this directive on specific options for establishing this capability, including recommendations for its organizational location and structure.

Vulnerability Assessments

(11) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall expand and continue vulnerability assessments of the agriculture and food sectors. These vulnerability assessments should identify requirements of the National Infrastructure Protection Plan developed by the Secretary of Homeland Security, as appropriate, and shall be updated every **2 years**.

Mitigation Strategies

(12) The Secretary of Homeland Security and the Attorney General, working with the Secretaries of Agriculture, Health and Human Services, the Administrator of the Environmental Protection Agency, the Director of Central Intelligence, and the heads of other appropriate Federal departments and agencies shall prioritize, develop, and implement, as appropriate, mitigation strategies to protect vulnerable critical nodes of production or processing from the introduction of diseases, pests, or poisonous agents.

(13) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall build on existing efforts to expand development of common screening and inspection procedures for agriculture and food items entering the United States and to maximize effective domestic inspection activities for food items within the United States.

Response Planning and Recovery

(14) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, the Attorney General, and the Administrator of the Environmental Protection Agency, will ensure that the combined Federal, State, and local response capabilities are adequate to respond quickly and effectively to a terrorist attack, major disease outbreak, or other disaster affecting the national agriculture or food infrastructure. These activities will be integrated with other national homeland security preparedness activities developed under HSPD-8 on National Preparedness.

(15) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, the Attorney General, and the Administrator of the Environmental Protection Agency, shall develop a coordinated agriculture and food-specific standardized response plan that will be integrated into the National Response Plan. This plan will ensure a coordinated response to an agriculture or food incident and will delineate the appropriate roles of Federal, State, local, and private sector partners, and will address risk communication for the general public.

(16) The Secretaries of Agriculture and Health and Human Services, in coordination with the Secretary of Homeland Security and the Administrator of the Environmental Protection Agency, shall enhance recovery systems that are able to stabilize agriculture production, the food supply, and the economy, rapidly remove and effectively dispose of contaminated agriculture and food products or infected plants and animals, and decontaminate premises.

(17) The Secretary of Agriculture shall study and make recommendations to the Homeland Security Council, within 120 days of the date of this directive, for the use of existing, and the creation of new, financial risk management tools encouraging self-protection for agriculture and food enterprises vulnerable to losses due to terrorism.

18) The Secretary of Agriculture, in coordination with the Secretary of Homeland Security, and in consultation with the Secretary of Health and Human Services and the Administrator of the Environmental Protection Agency, shall work with State and local governments and the private sector to develop:

(a) A National Veterinary Stockpile (NVS) containing sufficient amounts of animal vaccine, antiviral, or therapeutic products to appropriately respond to the most damaging animal diseases affecting human health and the economy and that will be capable of deployment within 24 hours of an outbreak. The NVS shall leverage where appropriate the mechanisms and infrastructure that have been developed for the management, storage, and distribution of the Strategic National Stockpile.

(b) A National Plant Disease Recovery System (NPDRS) capable of responding to a high-consequence plant disease with pest control measures and the use of resistant seed varieties within a single growing season to sustain a reasonable level of production for economically important crops. The NPDRS will utilize the genetic resources contained in the U.S. National Plant Germplasm System, as well as the scientific capabilities of the Federal-State-industry agricultural research and extension system. The NPDRS shall include emergency planning for the use of resistant seed varieties and pesticide control measures to prevent, slow, or stop the spread of a high-consequence plant disease, such as wheat smut or soybean rust.

Outreach and Professional Development

(19) The Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, and the heads of other appropriate Federal departments and agencies, shall work with appropriate private sector entities to establish an effective information sharing and analysis mechanism for agriculture and food.

(20) The Secretaries of Agriculture and Health and Human Services, in consultation with the Secretaries of Homeland Security and Education, shall support the development of and promote higher education programs for the protection of animal, plant, and public health. To the extent permitted by law and subject to availability of funds, the program will provide capacity building grants to colleges and schools of veterinary medicine, public health, and agriculture that design higher education training programs for veterinarians in exotic animal diseases, epidemiology, and public health as well as new programs in plant diagnosis and treatment.

(21) The Secretaries of Agriculture and Health and Human Services, in consultation with the Secretaries of Homeland Security and Education, shall support the development of and promote a higher education program to address protection of the food supply. To the extent permitted by law and subject to the availability of funds, the program will provide capacity-building grants to universities for interdisciplinary degree programs that combine training in food sciences, agriculture sciences, medicine, veterinary medicine, epidemiology, microbiology, chemistry, engineering, and mathematics (statistical modeling) to prepare food defense professionals.

(22) The Secretaries of Agriculture, Health and Human Services, and Homeland Security shall establish opportunities for professional development and specialized training in agriculture and food protection, such as internships, fellowships, and other post-graduate opportunities that provide for homeland security professional workforce needs.

Research and Development

(23) The Secretaries of Homeland Security, Agriculture, and Health and Human Services, the Administrator of the Environmental Protection Agency, and the heads of other appropriate Federal departments and agencies, in consultation with the Director of the Office of Science and Technology

Policy, will accelerate and expand development of current and new countermeasures against the intentional introduction or natural occurrence of catastrophic animal, plant, and zoonotic diseases. The Secretary of Homeland Security will coordinate these activities. This effort will include countermeasure research and development of new methods for detection, prevention technologies, agent characterization, and dose response relationships for high-consequence agents in the food and the water supply.

(24) The Secretaries of Agriculture and Homeland Security will develop a plan to provide safe, secure, and state-of-the-art agriculture biocontainment laboratories that research and develop diagnostic capabilities for foreign animal and zoonotic diseases.

(25) The Secretary of Homeland Security, in consultation with the Secretaries of Agriculture and Health and Human Services, shall establish university-based centers of excellence in agriculture and food security.

Budget

(26) For all future budgets, the Secretaries of Agriculture, Health and Human Services, and Homeland Security shall submit to the Director of the Office of Management and Budget, concurrent with their budget submissions, an integrated budget plan for defense of the United States food system.

Implementation

(27) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and Presidential guidance.

(28) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH

# # #

For Immediate Release
Office of the Press Secretary
The White House
August 27, 2004

August 27, 2004 Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH