COMPILATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVES (HSPD)

110TH CONGRESS
2nd Session

COMMITTEE PRINT

COMMITTEE
PRINT 110–B

COMPILATION

OF

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES (HSPD)

(Updated through December 31, 2007)

PREPARED FOR THE USE OF THE

COMMITTEE ON HOMELAND SECURITY

OF THE

HOUSE OF REPRESENTATIVES

JANUARY 2008

U.S. GOVERNMENT PRINTING OFFICE

39–618 PDF

WASHINGTON : 2008

110TH CONGRESS
2nd Session

COMMITTEE PRINT

COMMITTEE
PRINT 110–B

COMPILATION

OF

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES (HSPD)

(Updated through December 31, 2007)

PREPARED FOR THE USE OF THE

COMMITTEE ON HOMELAND SECURITY

OF THE

HOUSE OF REPRESENTATIVES

JANUARY 2008

U.S. GOVERNMENT PRINTING OFFICE

39–618 PDF

WASHINGTON : 2008

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
DONNA M. CHRISTENSEN, Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey
PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia

Jessica Herrera-Flanigan, *Staff Director & General Counsel*
Rosaline Cohen, *Chief Counsel*
Michael S. Twinchek, *Chief Clerk*
Robert O'Connor, *Minority Staff Director*

CONTENTS

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—1

ORGANIZATION AND OPERATION OF THE HOMELAND SECURITY COUNCIL

OCTOBER 29, 2001

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 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 CentralIntelligence; 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 Cyberspace 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 andPlans);
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

COMBATING TERRORISM THROUGH IMMIGRATION POLICIES

OCTOBER 29, 2001

(AS AMENDED BY HSPD—5**)**

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 TrackingTask 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)**]** the Department of Homeland Security 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 Investigation, 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, the Secretary of Homeland Security, 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, the Secretary of Homeland Security, 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] Secretary of Homeland Security, 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] Department of Homeland Security. 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] Department of Homeland Security special agents assigned to Joint Terrorism Task Forces, as deemed appropriate by the Attorney General and the [Secretary of the Treasury] Secretary of Homeland Security. These officers shall constitute new positions over and above the existing on-duty special agent forces of the [two agencies] Department of Homeland Security.

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, the Secretary of Homeland Security, 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 Department of State, the Department of Homeland Security, 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 Secretary of Homeland Security, 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] Department of Homeland Security, 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] Homeland Security 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] Homeland Security 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] Homeland Security, 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]Homeland Security 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, the Secretary of Homeland Security, 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 governments, 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

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—3

HOMELAND SECURITY ADVISORY SYSTEM

MARCH 11, 2007

(AS AMENDED BY HSPD—5)

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**]** Secretary of Homeland Security in consultation with the Assistant to the President for Homeland Security. **[**Except in exigent circumstances, the At-

torney 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.] 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. 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 responsible 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] Secretary of Homeland Security 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] Secretary of Homeland Security 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] Secretary of Homeland Security 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.

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.

The Director of Central Intelligence, the Secretary of Homeland Security 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 prepositioning 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

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—4

(National Security Presidential Directive—17)

NATIONAL STRATEGY TO COMBAT WEAPONS OF MASS DESTRUCTION

DECEMBER 11, 2004
{UNCLASSIFIED VERSION}

"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

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.

2Consequence 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 hor-

rific 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-5

MANAGEMENT OF DOMESTIC INCIDENTS

FEBRUARY 28, 2003

(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 operational 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—6

INTEGRATION AND USE OF SCREENING INFORMATION
SEPTEMBER 16, 2003

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 direc-

tive, 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—7

CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION

DECEMBER 17, 2003

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 ex-

ploit 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 prin-

cipal 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 Sec-

retaries 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—8

NATIONAL PREPAREDNESS

DECEMBER 17, 2003

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 Sec-

retary, 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 nongovernmental 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

HOMELAND SECURITY PRESIDENTIAL—9

DEFENSE OF UNITED STATES AGRICULTURE AND FOOD

JANUARY 30, 2004

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 Serv-

ices, 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 relation-

ships 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

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—10

BIODEFENSE FOR THE 21ST CENTURY

APRIL 28, 2004

"Bioterrorism is a real threat to our country. It's a threat to every nation that loves freedom. Terrorist groups seek biological weapons; we know some rogue states already have them....It's important that we confront these real threats to our country and prepare for future emergencies."

President George W. Bush
June 12, 2002

"Armed with a single vial of a biological agent small groups of fanatics, or failing states, could gain the power to threaten great nations, threaten the world peace. America, and the entire civilized world, will face this threat for decades to come. We must confront the danger with open eyes, and unbending purpose."

President Bush
February 11, 2004

Biological weapons in the possession of hostile states or terrorists pose unique and grave threats to the safety and security of the United States and our allies. Biological weapons attacks could cause catastrophic harm. They could inflict widespread injury and result in massive casualties and economic disruption. Bioterror attacks could mimic naturally-occurring disease, potentially delaying recognition of an attack and creating uncertainty about whether one has even occurred. An attacker may thus believe that he could escape identification and capture or retaliation.

Biological weapons attacks could be mounted either inside or outside the United States and, because some biological weapons agents are contagious, the effects of an initial attack could spread widely. Disease outbreaks, whether natural or deliberate, respect no geographic or political borders.

Preventing and controlling future biological weapons threats will be even more challenging. Advances in biotechnology and life sciences - including the spread of expertise to create modified or novel organisms - present the prospect of new toxins, live agents, and bioregulators that would require new detection methods, preventive measures, and treatments. These trends increase the risk for surprise. Anticipating such threats through intelligence efforts is made more difficult by the dual-use nature of biological tech-

nologies and infrastructure, and the likelihood that adversaries will use denial and deception to conceal their illicit activities. The stakes could not be higher for our Nation. Attacks with biological weapons could:

- Cause catastrophic numbers of acute casualties, long-term disease and disability, psychological trauma, and mass panic;
- Disrupt critical sectors of our economy and the day-to-day lives of Americans; and
- Create cascading international effects by disrupting and damaging international trade relationships, potentially globalizing the impacts of an attack on United States soil.

Fortunately, the United States possesses formidable capabilities to mount credible biodefenses. We have mobilized our unrivaled biomedical research infrastructure and expanded our international research relationships. In addition, we have an established medical and public health infrastructure that is being revitalized and expanded. These capabilities provide a critical foundation on which to build improved and comprehensive biodefenses.

The United States has pursued aggressively a broad range of programs and capabilities to confront the biological weapons threat. These actions, taken together, represent an extraordinary level of effort by any measure. Among our significant accomplishments, we have:

- Expanded international efforts to keep dangerous biological materials out of the hands of terrorists;
- Launched the Proliferation Security Initiative to stem the trafficking in weapons of mass destruction (WMD), including biological weapons;
- Established the BioWatch program, a network of environmental sensors to detect biological weapons attacks against major cities in the United States;
- Initiated new programs to secure and defend our agriculture and food systems against biological contamination;
- Increased funding for bioterrorism research within the Department of Health and Human Services by thirty-fold;
- Expanded the Strategic National Stockpile of medicines for treating victims of bioterror attacks, ensuring that the stockpile's "push packages" can be anywhere in the United States within 12 hours;
- Stockpiled enough smallpox vaccine for every American, and vaccinated over 450,000 members of the armed services;
- Launched and funded Project BioShield to speed the development and acquisition of new medical countermeasures against biological weapons;
- Provided Federal funds to improve the capacities of state and local health systems to detect, diagnose, prevent, and respond to biological weapons attacks; and
- Worked with the international community to strengthen global, regional and national programs to prevent, detect, and respond to biological weapons attacks.

Building on these accomplishments, we conducted a comprehensive evaluation of our biological defense capabilities to identify future priorities and actions to support them. The results of

that study provide a blueprint for our future biodefense program, Biodefense for the 21st Century, that fully integrates the sustained efforts of the national and homeland security, medical, public health, intelligence, diplomatic, and law enforcement communities.

Specific direction to departments and agencies to carry out this biodefense program is contained in a classified version of this directive.

Biodefense for the 21st Century

The United States will continue to use all means necessary to prevent, protect against, and mitigate biological weapons attacks perpetrated against our homeland and our global interests. Defending against biological weapons attacks requires us to further sharpen our policy, coordination, and planning to integrate the biodefense capabilities that reside at the Federal, state, local, and private sector levels. We must further strengthen the strong international dimension to our efforts, which seeks close international cooperation and coordination with friends and allies to maximize our capabilities for mutual defense against biological weapons threats.

While the public health philosophy of the 20th Century emphasizing prevention is ideal for addressing natural disease outbreaks, it is not sufficient to confront 21st Century threats where adversaries may use biological weapons agents as part of a long-term campaign of aggression and terror. Health care providers and public health officers are among our first lines of defense. Therefore, we are building on the progress of the past three years to further improve the preparedness of our public health and medical systems to address current and future BW threats and to respond with greater speed and flexibility to multiple or repetitive attacks.

Private, local, and state capabilities are being augmented by and coordinated with Federal assets, to provide layered defenses against biological weapons attacks. These improvements will complement and enhance our defense against emerging or reemerging natural infectious diseases.

The traditional approach toward protecting agriculture, food, and water - focusing on the natural or unintentional introduction of a disease - also is being greatly strengthened by focused efforts to address current and anticipated future biological weapons threats that may be deliberate, multiple, and repetitive.

Finally, we are continuing to adapt United States military forces to meet the biological weapons challenge. We have long recognized that adversaries may seek biological weapons to overcome our conventional strength and to deter us from responding to aggression. A demonstrated military capability to defend against biological weapons and other WMD strengthens our forward military presence in regions vital to United States security, promotes deterrence, and provides reassurance to critical friends and allies. The Department of Defense will continue to ensure that United States military forces can operate effectively in the face of biological weapons attacks, and that our troops and our critical domestic and overseas installations are effectively protected against such threats.

Pillars of Our Biodefense Program

The essential pillars of our national biodefense program are: Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery.

Successful implementation of our program requires optimizing critical cross-cutting functions such as: information management and communications; research development and acquisition; creation and maintenance of needed biodefense infrastructure, including the human capital to support it; public preparedness; and strengthened bilateral, multilateral, and international cooperation.

National biodefense preparedness and response requires the involvement of a wide range of Federal departments and agencies. The Secretary of Homeland Security is the principal Federal official for domestic incident management and is responsible for coordinating domestic Federal operations to prepare for, respond to, and recover from biological weapons attacks. The Secretary of Homeland Security coordinates, as appropriate, with the heads of other Federal departments and agencies, to effectively accomplish this mission.

The Secretary of State is the principal Federal officer responsible for international terrorist incidents that take place outside the U.S. territory, including United States support for foreign consequence management and coordinates, as appropriate, with heads of other Federal departments and agencies, to effectively accomplish this mission. When requested by the Secretary of State, and approved by the Secretary of Defense, the Department of Defense will support United States foreign consequence management operations, as appropriate.

The following sections describe our aims and objectives for further progress under each of the pillars of our national biodefense program, as well as highlight key roles played by Federal departments and agencies.

Threat Awareness Biological Warfare Related Intelligence

Timely, accurate, and relevant intelligence enables all aspects of our national biodefense program. Despite the inherent challenges of identifying and characterizing biological weapons programs and anticipating biological attacks, we are improving the Intelligence Community's ability to collect, analyze, and disseminate intelligence. We are increasing the resources dedicated to these missions and adopting more aggressive approaches for accomplishing them. Among our many initiatives, we are continuing to develop more forward-looking analyses, to include Red Teaming efforts, to understand new scientific trends that may be exploited by our adversaries to develop biological weapons and to help position intelligence collectors ahead of the problem.

Assessments

Another critical element of our biodefense policy is the development of periodic assessments of the evolving biological weapons threat. First, the United States requires a continuous, formal process for conducting routine capabilities assessments to guide prioritization of our on-going investments in biodefense-related research, development, planning, and preparedness. These assessments will be tailored to meet the requirements in each of these areas. Second, the United States requires a periodic senior-level

policy net assessment that evaluates progress in implementing this policy, identifies continuing gaps or vulnerabilities in our biodefense posture, and makes recommendations for re-balancing and refining investments among the pillars of our overall biodefense policy. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, will be responsible for conducting these assessments.

Anticipation of Future Threats

The proliferation of biological materials, technologies, and expertise increases the potential for adversaries to design a pathogen to evade our existing medical and non-medical countermeasures. To address this challenge, we are taking advantage of these same technologies to ensure that we can anticipate and prepare for the emergence of this threat. We are building the flexibility and speed to characterize such agents, assess existing defenses, and rapidly develop safe and effective countermeasures. In addition, we must guard against the spread of potentially infectious agents from beyond our borders. We are strengthening the ability of our medical, public health, agricultural, defense, law enforcement, diplomatic, environmental, and transportation infrastructures to recognize and confront such threats and to contain their impact. The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, is working to ensure an integrated and focused national effort to anticipate and respond to emerging biological weapons threats.

Prevention and Protection

Proactive Prevention

Preventing biological weapons attacks is by far the most cost-effective approach to biodefense. Prevention requires the continuation and expansion of current multilateral initiatives to limit the access of agents, technology, and know-how to countries, groups, or individuals seeking to develop, produce, and use these agents.

To address this challenge, we are further enhancing diplomacy, arms control, law enforcement, multilateral export controls, and threat reduction assistance that impede adversaries seeking biological weapons capabilities. Federal departments and agencies with existing authorities will continue to expand threat reduction assistance programs aimed at preventing the proliferation of biological weapons expertise. We will continue to build international coalitions to support these efforts, encouraging increased political and financial support for nonproliferation and threat reduction programs. We will also continue to expand efforts to control access and use of pathogens to strengthen security and prevention.

The National Strategy to Combat Weapons of Mass Destruction, released in December 2002, places special emphasis on the need for proactive steps to confront WMD threats. Consistent with this approach, we have improved and will further improve our ability to detect and destroy an adversary's biological weapons assets before they can be used. We are also further expanding existing capabilities to interdict enabling technologies and materials, including through the Proliferation Security Initiative. Additionally, we are working to improve supporting intelligence capabilities to pro-

vide timely and accurate information to support proactive prevention.

Responsibilities for proactive prevention are wide-ranging, with the Department of State, Department of Defense, Department of Justice, and the Intelligence Community playing critical roles in our overall government-wide effort.

Critical Infrastructure Protection

Protecting our critical infrastructure from the effects of biological weapons attacks is a priority. A biological weapons attack might deny us access to essential facilities and response capabilities. Therefore, we are working to improve the survivability and ensure the continuity and restoration of operations of critical infrastructure sectors following biological weapons attacks. Assessing the vulnerability of this infrastructure, particularly the medical, public health, food, water, energy, agricultural, and transportation sectors, is the focus of current efforts. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, leads these efforts, which include developing and deploying biodetection technologies and decontamination methodologies.

Surveillance and Detection

Attack Warning

Early warning, detection, or recognition of biological weapons attacks to permit a timely response to mitigate their consequences is an essential component of biodefense. Through the President's recently proposed biosurveillance initiative, the United States is working to develop an integrated and comprehensive attack warning system to rapidly recognize and characterize the dispersal of biological agents in human and animal populations, food, water, agriculture, and the environment. Creating a national bioawareness system will permit the recognition of a biological attack at the earliest possible moment and permit initiation of a robust response to prevent unnecessary loss of life, economic losses, and social disruption. Such a system will be built upon and reinforce existing Federal, state, local, and international surveillance systems. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, integrates these efforts.

Attribution

Deterrence is the historical cornerstone of our defense, and attribution - the identification of the perpetrator as well as method of attack .- forms the foundation upon which deterrence rests. Biological weapons, however, lend themselves to covert or clandestine attacks that could permit the perpetrator to remain anonymous. We are enhancing our deterrence posture by improving attribution capabilities. We are improving our capability to perform technical forensic analysis and to assimilate all-source information to enable attribution assessments. We have created and designated the National Bioforensic Analysis Center of the National Biodefense Analysis and Countermeasure Center, under the Department of Homeland Security, as the lead Federal facility to conduct and facilitate the technical forensic analysis and interpretation of materials re-

covered following a biological attack in support of the appropriate lead Federal agency.

Response and Recovery

Once a biological weapons attack is detected, the speed and coordination of the Federal, state, local, private sector, and international response will be critical in mitigating the lethal, medical, psychological, and economic consequences of such attacks. Responses to biological weapons attacks depend on pre-attack planning and preparedness, capabilities to treat casualties, risk communications, physical control measures, medical countermeasures, and decontamination capabilities.

Response Planning

A biological response annex is being drafted as part of our National Response Plan (NRP). We are catalyzing the development of state and local plans that are consistent with the NRP and ensure a seamless coordinated effort. Capabilities required for response and mitigation against biological attacks will be based on interagency-agreed scenarios that are derived from plausible threat assessments. These plans will be regularly tested as part of Federal, state, local, and international exercises. The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, is developing comprehensive plans that provide for seamless, coordinated Federal, state, local, and international responses to a biological attack.

Mass Casualty Care

Following a biological weapons attack, all necessary means must be rapidly brought to bear to prevent loss of life, illness, psychological trauma, and to contain the spread of potentially contagious diseases. Provision of timely preventive treatments such as antibiotics or vaccines saves lives, protects scarce medical capabilities, preserves social order, and is cost effective.

The Administration is working closely with state and local public health officials to strengthen plans to swiftly distribute needed medical countermeasures. Moreover, we are working to expand and, where needed, create new Federal, state, and local medical and public health capabilities for all-hazard mass casualty care.

The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, is the principal Federal agency responsible for coordinating all Federal-level assets activated to support and augment the state and local medical and public health response to mass casualty events. For those mass casualty incidents that require parallel deployment of Federal assets in other functional areas such as transportation or law enforcement, the Department of Homeland Security will coordinate the overall Federal response in accordance with its statutory authorities for domestic incident management. Under certain circumstances, the Department of Veterans Affairs and the Department of Defense, given their specialized expertise and experience, may be called upon to play important supporting roles in mass casualty care.

Risk Communication

A critical adjunct capability to mass casualty care is effective risk communication. Timely communications with the general public and the medical and public health communities can significantly influence the success of response efforts, including health- and life-sustaining interventions. Efforts will be made to develop communication strategies, plans, products, and channels to reach all segments of our society, including those with physical or language limitations. These efforts will ensure timely domestic and international dissemination of information that educates and reassures the general public and relevant professional sectors before, during, and after an attack or other public health emergency.

The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, is developing comprehensive coordinated risk communication strategies to facilitate emergency preparedness for biological weapons attacks. This includes travel and citizen advisories, international coordination and communication, and response and recovery communications in the event of a large-scale biological attack.

Medical Countermeasure Development

Development and deployment of safe, effective medical countermeasures against biological weapons agents of concern remains an urgent priority. The National Institutes of Health (NIH), under the direction of the Department of Health and Human Services, is working with the Department of Homeland Security, the Department of Defense, and other agencies to shape and execute an aggressive research program to develop better medical countermeasures. NIH.s work increasingly will reflect the potential for novel or genetically engineered biological weapons agents and possible scenarios that require providing broad-spectrum coverage against a range of possible biological threats to prevent illness even after exposure. Additionally, we have begun construction of new labs. We are striving to assure the nation has the infrastructure required to test and evaluate existing, proposed, or promising countermeasures, assess their safety and effectiveness, expedite their development, and ensure rapid licensure.

The Department of Health and Human Services, in coordination with other appropriate Federal departments and agencies, will continue to ensure the development and availability of sufficient quantities of safe and efficacious medical countermeasures to mitigate illness and death in the event of a biological weapons attack.

Decontamination

Recovering from a biological weapons attack may require significant decontamination and remediation activities. We are working to improve Federal capabilities to support states and localities in their efforts to rapidly assess, decontaminate, and return to preattack activities, and are developing standards and protocols for the most effective approaches for these activities.

The Administrator of the Environmental Protection Agency, in coordination with the Attorney General and the Secretaries of Defense, Agriculture, Labor, Health and Human Services, and Homeland Security, is developing specific standards, protocols, and capabilities to address the risks of contamination following a biological

weapons attack and developing strategies, guidelines, and plans for decontamination of persons, equipment, and facilities.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—11

COMPREHENSIVE TERRORIST-RELATED SCREENING PROCEDURES

AUGUST 27, 2004

---

(1) In order more effectively to detect and interdict individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("suspected terrorists") and terrorist activities, it is the policy of the United States to:

(a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and

(b) implement a coordinated and comprehensive approach to terrorist-related screening - in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure - that supports homeland security, at home and abroad.

(2) This directive builds upon HSPD-6, "Integration and Use of Screening Information to Protect Against Terrorism." The Terrorist Screening Center (TSC), which was established and is administered by the Attorney General pursuant to HSPD-6, enables Government officials to check individuals against a consolidated Terrorist Screening Center Database. Other screening activities underway within the Terrorist Threat Integration Center (TTIC) and the Department of Homeland Security further strengthen the ability of the United States Government to protect the people, property, and territory of the United States against acts of terrorism.

(3) In this directive, the term "terrorist-related screening" means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-

related screening also includes risk assessment, inspection, and credentialing.

(4) Not later than 75 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and the Office of Management and Budget, and the heads of other appropriate Federal departments and agencies, shall submit to me, through the Assistant to the President for Homeland Security, a report setting forth plans and progress in the implementation of this directive, including as further described in sections 5 and 6 of this directive.

(5) The report shall outline a strategy to enhance the effectiveness of terrorist-related screening activities, in accordance with the policy set forth in section 1 of this directive, by developing comprehensive, coordinated, systematic terrorist-related screening procedures and capabilities that also take into account the need to:

(a) maintain no less than current levels of security created by existing screening and protective measures;

(b) encourage innovations that exceed established standards;

(c) ensure sufficient flexibility to respond rapidly to changing threats and priorities;

(d) permit flexibility to incorporate advancements into screening applications and technology rapidly;

(e) incorporate security features, including unpredictability, that resist circumvention to the greatest extent possible;

(f) build upon existing systems and best practices and, where appropriate, integrate, consolidate, or eliminate duplicative systems used for terrorist-related screening;

(g) facilitate legitimate trade and travel, both domestically and internationally;

(h) limit delays caused by screening procedures that adversely impact foreign relations, or economic, commercial, or scientific interests of the United States; and

(i) enhance information flow between various screening programs.

(6) The report shall also include the following:

(a) the purposes for which individuals will undergo terrorist-related screening;

(b) a description of the screening opportunities to which terrorist-related screening will be applied;

(c) the information individuals must present, including, as appropriate, the type of biometric identifier or other form of identification or identifying information to be presented, at particular screening opportunities;

(d) mechanisms to protect data, including during transfer of information;

(e) mechanisms to address data inaccuracies, including names inaccurately contained in the terrorist screening data consolidated pursuant to HSPD-6;

(f) the procedures and frequency for screening people, cargo, and conveyances;

(g) protocols to support consistent risk assessment and inspection procedures;

(h) the skills and training required for the screeners at screening opportunities;

(i) the hierarchy of consequences that should occur if a risk indicator is generated as a result of a screening opportunity;

(j) mechanisms for sharing information among screeners and all relevant Government agencies, including results of screening and new information acquired regarding suspected terrorists between screening opportunities;

(k) recommended research and development on technologies designed to enhance screening effectiveness and further protect privacy interests; and

(l) a plan for incorporating known traveler programs into the screening procedures, where appropriate.

(7) Not later than 90 days after the date of this directive, the Secretary of Homeland Security, in coordination with the heads of the Federal departments and agencies listed in section 4 of this directive, shall also provide to me, through the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget, a prioritized investment and implementation plan for a systematic approach to terrorist-related screening that optimizes detection and interdiction of suspected terrorists and terrorist activities. The plan shall describe the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement the policy set forth in section 1 of this directive. The Secretary of Homeland Security shall further provide a report on the status of the implementation of the plan to me through the Assistant to the President for Homeland Security 6 months after the date of this directive and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

(8) In order to ensure comprehensive and coordinated terrorist-related screening procedures, the implementation of this directive shall be consistent with Government-wide efforts to improve information sharing. Additionally, the reports and plan required under sections 4 and 7 of this directive shall inform development of Government-wide information sharing improvements.

(9) This directive does not alter existing authorities or responsibilities of department and agency heads including to carry out operational activities or provide or receive information. 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.

GEORGE W. BUSH

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—12

POLICY FOR A COMMON IDENTIFICATION STANDARD FOR FEDERAL EMPLOYEES AND CONTRACTORS

AUGUST 27, 2004

---

(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

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—13

(NATIONAL SECURITY PRESIDENTIAL DIRECTIVE—41)

MARITIME SECURITY POLICY

DECEMBER 21, 2004

Memorandum for
The Vice President
The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Attorney General
The Secretary of the Interior
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
The Secretary of Homeland Security
Chief of Staff to the President
Director, Office of Management and Budget
The United States Trade Representative
Assistant to the President for National Security Affairs
Counsel to the President
Assistant to the President for Homeland Security
Chairman, Council on Environmental Quality
Director of Central Intelligence
Chairman of the Joint Chiefs of Staff
Commandant of the Coast Guard
Director, Federal Bureau of Investigation
Director, National Counterterrorism Center

This directive establishes U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests. It directs the coordination of United States Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities. This directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts. As specified herein, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security, in cooperation with appropriate Federal departments and agencies, will jointly coordinate the implementation of the policy set forth in Section II of this directive.

I. BACKGROUND

For the purposes of this directive, "Maritime Domain" means all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. Due to its complex nature and immense size, the Maritime Domain is particularly susceptible to exploitation and disruption by individuals, organizations, and States. The Maritime Domain facilitates a unique freedom of movement and flow of goods while allowing people, cargo, and conveyances to transit with anonymity not generally available by movement over land or by air. Individuals and organizations hostile to the United States have demonstrated a continuing desire to exploit such vulnerabilities. The United States must deploy the full range of its operational assets and capabilities to prevent the Maritime Domain from being used by terrorists, criminals, and hostile States to commit acts of terrorism and criminal or other unlawful or hostile acts against the United States, its people, economy, property, territory, allies, and friends, while recognizing that maritime security policies are most effective when the strategic importance of international trade, economic cooperation, and the free flow of commerce are considered appropriately.

II. POLICY

The security of the Maritime Domain is a global issue. The United States, in cooperation with our allies and friends around the world and our State, local, and private sector partners, will work to ensure that lawful private and public activities in the Maritime Domain are protected against attack and criminal and otherwise unlawful or hostile exploitation. These efforts are critical to global economic stability and growth and are vital to the interests of the United States.

It is the policy of the United States to take all necessary and appropriate actions, consistent with U.S. law, treaties and other international agreements to which the United States is a party, and customary international law as determined for the United States by the President, to enhance the security of and protect U.S. interests in the Maritime Domain, including the following:

- Preventing terrorist attacks or criminal acts or hostile acts in, or the unlawful exploitation of, the Maritime Domain, and reducing the vulnerability of the Maritime Domain to such acts and exploitation;
- Enhancing U.S. national security and homeland security by protecting U.S. population centers, critical infrastructure, borders, harbors, ports, and coastal approaches in the Maritime Domain;
- Expediting recovery and response from attacks within the Maritime Domain;
- Maximizing awareness of security issues in the Maritime Domain in order to support U.S. forces and improve United States Government actions in response to identified threats;

• Enhancing international relationships and promoting the integration of U.S. allies and international and private sector partners into an improved global maritime security framework to advance common security interests in the Maritime Domain; and

• Ensuring seamless, coordinated implementation of authorities and responsibilities relating to the security of the Maritime Domain by and among Federal departments and agencies. These actions must be undertaken in a manner that facilitates global commerce and preserves the freedom of the seas for legitimate military and commercial navigation and other legitimate activities as well as civil liberties and the rights guaranteed under the Constitution.

III. POLICY COORDINATION

The Maritime Security Policy Coordinating Committee (MSPCC) is hereby established, consistent with NSPD-1 and HSPD-1. The MSPCC, in consultation with the relevant regional and functional policy coordinating committees of the Federal Government, and without exercising operational oversight, shall act as the primary forum for interagency coordination of the implementation of this directive. As part of that effort, the MSPCC shall review existing interagency practices, coordination, and execution of U.S. policies and strategies relating to maritime security, and shall recommend specific improvements to all of them as warranted. The MSPCC shall provide analysis of new U.S. policies, strategies, and initiatives relating to maritime security for consideration by the Deputies and Principals Committees of the NSC and the HSC, and subsequently by the NSC and the HSC, and shall ensure ongoing coordination and implementation of such policies, strategies, and initiatives.

The reviews, plans, and recommendations required by this directive (as set forth in Sections IV and V below) shall be completed by the departments and agencies designated herein in coordination with the MSPCC, and shall then be prepared for consideration by and submitted to the Deputies and Principals Committees of the NSC and the HSC, and subsequently to the NSC and the HSC.

The MSPCC shall be co-chaired by an NSC staff representative selected by the Assistant to the President for National Security Affairs and an HSC representative selected by the Assistant to the President for Homeland Security, and shall include the following officers or their designated representatives:

- The Vice President
- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Attorney General
- The Secretary of the Interior
- The Secretary of Commerce
- The Secretary of Transportation
- The Secretary of Energy
- The Secretary of Homeland Security
- Director, Office of Management and Budget

- The United States Trade Representative
- Chairman of the Council on Environmental Quality
- Director of Central Intelligence
- Chairman of the Joint Chiefs of Staff
- Director, Federal Bureau of Investigation
- Director, National Counterterrorism Center

The co-chairs of the MSPCC may invite representatives of other departments and agencies to attend MSPCC meetings as they deem appropriate.

IV. POLICY IMPLEMENTATION

National Strategy for Maritime Security.

A coordinated and integrated government-wide effort to enhance the security of the Maritime Domain requires an over-arching strategy. The Secretaries of Defense and Homeland Security shall jointly lead a collaborative interagency effort to draft a recommended National Strategy for Maritime Security, which shall be submitted for my consideration within 180 days after the effective date of this directive. Such a strategy must present an over-arching plan to implement this directive and address all of the components of the Maritime Domain, including domestic, international, public, and private components. It shall further incorporate a global, cross-discipline approach to the Maritime Domain centered on a layered, defense-in-depth framework that may be adjusted based on the threat level. The strategy shall build on current efforts and those initiated by this directive, as well as complement existing strategies, tools, and resources. All relevant Federal departments and agencies shall cooperate with the Secretaries of Defense and Homeland Security in this effort and provide all appropriate assistance.

V. POLICY ACTIONS

In concert with the development of a National Strategy for Maritime Security, the following actions shall be taken: Maritime Domain Awareness (MDA). Maritime Domain Awareness is the effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy, or environment of the United States. It is critical that the United States develop an enhanced capability to identify threats to the Maritime Domain as early and as distant from our shores as possible by integrating intelligence, surveillance, observation, and navigation systems into a common operating picture accessible throughout the United States Government.

The Secretaries of Defense and Homeland Security have established a Maritime Domain Awareness Senior Steering Group (MDASSG). The MDASSG is co-chaired by representatives of the Secretaries of Defense and Homeland Security and includes representatives from departments and agencies that will participate in the MSPCC.

The MDASSG shall coordinate national efforts to achieve maximum Maritime Domain Awareness. No later than 180 days after the effective date of this directive, the MDASSG will develop and submit to me, through the Secretaries of Defense and Homeland Security, a national plan to improve Maritime

Domain Awareness, which shall include near-term and long-term objectives, required program and resource implications, and any recommendations for organizational or policy changes.

Global Maritime Intelligence Integration.

A robust and coordinated intelligence effort serves as the foundation for effective security efforts in the Maritime Domain. In support of this effort, I direct the Secretaries of Defense and Homeland Security, with the support of the Director of Central Intelligence, and in coordination with the Director of the National Counterterrorism Center (NCTC) and the Director of the Federal Bureau of Investigation (FBI), to use existing intelligence capabilities to integrate all available intelligence on a global basis regarding the location, identity, and operational capabilities and intentions of potential threats to U.S. interests in the Maritime Domain. The Secretaries of Defense and Homeland Security, with the support of the Director of Central Intelligence, and in coordination with the Director of the NCTC, the Director of the FBI, and other appropriate departments and agencies, shall submit to me for approval, through the Assistants to the President for National Security Affairs and Homeland Security, a plan for global maritime intelligence integration within 180 days after the effective date of this directive. The plan shall include appropriate interagency participation to ensure effective government-wide sharing of information and data critical to intelligence production.

Domestic Outreach.

A successful strategy to implement this directive must include coordination with State and local authorities and consultation with appropriate private sector persons and entities. The Secretary of Homeland Security, in coordination with the Attorney General and the Secretaries of the Treasury, Interior, Commerce, and Transportation, shall lead the development of a comprehensive engagement plan that ensures that the interests of State and local governments and the private sector are considered in the Federal Government's implementation of this directive. The plan shall be completed within 180 days after the effective date of this directive and shall take effect upon approval by the Secretary of Homeland Security.

Coordination of International Efforts and International Outreach.

Ensuring the security of the Maritime Domain must be a global effort, in which United States Government efforts are developed and furthered with the support of other governments and international organizations resulting in lasting international cooperation. The Secretary of State shall lead the coordination of United States Government initiatives in the implementation of this directive with regard to activities with foreign governments and international organizations. All Federal departments and agencies shall coordinate with the Department of State on policies, programs, and initiatives relating to the implementation of this directive that could affect the conduct of foreign policy. In addition, the Secretary of State, in coordination with the Secretaries of Defense, Commerce, Trans-

portation, and Homeland Security, and the U.S. Trade Representative, and in consultation with appropriate private sector persons and entities, shall develop, within 180 days after the effective date of this directive, a comprehensive plan to solicit international support for an improved global maritime security framework. Such plan shall take effect upon approval by the Secretary of State.

Maritime Threat Response.

The Secretaries of Defense and Homeland Security, in consultation with the Attorney General and the Secretaries of State, the Treasury, Commerce, and Transportation, shall develop a comprehensive National Maritime Security Response Plan to ensure seamless United States Government response to maritime threats against the United States. This plan, when approved by me, shall supplement the National Response Plan required by HSPD-5 and complement the critical infrastructure protection plans required by HSPD-7 and the domestic all-hazards preparedness goals and structures required by HSPD-8. The plan, at a minimum, shall reflect lead agency roles and responsibilities, including recommendations regarding changes to existing policy, including those reflected in PDD-39 and PDD-62, in the following areas:

1) maritime security response and counterterrorism operations;

2) maritime interception operations;

3) prevention and detection of, and response to, the mining of U.S. ports;

4) detection, interdiction and disposition of targeted cargo, people, and vessels; and

5) attacks on vessels with U.S. citizens aboard or that affect U.S. interests anywhere in the world.

The plan also shall:

1) include recommended protocols that establish clear coordination relationships governing protection and defense of the United States against threats to its interests in the Maritime Domain; and

2) provide recommendations concerning the designation of an interagency planning and command-and-control entity to ensure unity of command for national execution of maritime security policy. An interim plan shall be submitted no later than 180 days after the effective date of this directive, through the Assistants to the President for National Security Affairs and Homeland Security, and shall be finalized after completion of the National Strategy for Maritime Security.

Maritime Infrastructure Recovery.

Rapid recovery from an attack or similar disruption in the Maritime Domain is critical to the economic well-being of our Nation. A credible capability for rapid recovery will not only minimize an incident's economic impact but also serve as a deterrent. The Secretary of Homeland Security, in coordination with other appropriate officials, including the Secretaries of Defense, State, the Treasury, the Interior, Commerce, and

Transportation, and in consultation with key industry stakeholders, shall be responsible for the development of recommended minimum Federal standards, where appropriate, for maritime recovery operations, and shall develop comprehensive national maritime infrastructure recovery standards and a plan, complementary to the national preparedness goals and standards required by HSPD-8. Such standards and plan shall be completed no later than 180 days after the effective date of this directive, shall focus on the restoration of physical assets and transportation systems, and shall take effect when approved by the Secretary of Homeland Security. The standards and plan also shall describe a maritime infrastructure recovery exercise program consistent with the National Exercise Program administered by the Department of Homeland Security. The program shall address coordination with State, local, and private sector partners, and cooperation with foreign governments and international entities as appropriate.

Maritime Transportation System Security.

The Secretary of Homeland Security, in coordination with the Secretaries of Defense, State, Commerce, and Transportation, and the U.S. Trade Representative, and in consultation with appropriate industry representatives, shall develop recommendations for improvements to the national and international regulatory framework with respect to licensing, carriage, communications, safety equipment, and other critical systems for all private vessels, including commercial vessels, operating in the Maritime Domain.The recommendations shall be submitted to me, through the Assistants to the President for National Security Affairs and Homeland Security, no later than 180 days after the effective date of this directive.

Maritime Commerce Security.

To implement this directive effectively and to enhance economic growth, the United States must promote global supply chain security practices to reduce the risk of terrorists or criminals acting against the United States from within the Maritime Domain. The Secretary of Homeland Security, in coordination with the Secretaries of Defense, State, the Treasury, Commerce, Transportation, and Energy and the U.S. Trade Representative shall lead a collaborative interagency effort, in consultation with appropriate industry representatives, to develop a comprehensive international maritime supply chain security plan no later than 180 days after the effective date of this directive. The plan shall define supply-chain security requirements, include recommendations to further secure commercial operations from point of origin to point of destination, build on available resources, and provide a recommended framework of roles, responsibilities, and implementation actions. The plan shall define measurable national "end state" supply chain security goals and develop contingency plans to continue the flow of commerce in the event of an incident necessitating total or partial closure of U.S. borders to maritime

commerce. The plan shall take effect upon approval by the Secretary of Homeland Security.

VI. GENERAL.

This directive does not alter existing authorities or responsibilities of the department and agency heads, including their authorities, to carry out operational activities or to 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.

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 and Commander-in-Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

The Assistants to the President for National Security Affairs and Homeland Security and the Chairman of the Council on Environmental Quality shall coordinate as appropriate the work of the MSPCC under this directive and the work of the Committee on Ocean Policy under the Executive Order of December 17, 2004.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—14

(NATIONAL SECURITY PRESIDENTIAL DIRECTIVE—43)

DOMESTIC NUCLEAR DETECTION

APRIL 15, 2005

---

(1) To protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using such devices or materials against the people, territory, or interests of the United States, it is the policy of the United States to:

(a) Continue to develop, deploy, and enhance national nuclear and radiological detection capabilities in an effort to better detect, report on, disrupt, and prevent attempts to import, possess, store, transport, develop, or use such devices and materials;

(b) Continue to enhance the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response; and

(c) Continue to advance the science of nuclear and radiological detection through an aggressive, expedited, evolutionary, and transformational program of research and development in such detection technologies.

(2) To implement the policy set forth in paragraph (1), the Secretary of Homeland Security, in coordination with the Secretaries of State, Defense, and Energy, and the Attorney General, shall establish a national level Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security. The DNDO shall include personnel from the departments of Homeland Security (DHS), Defense (DOD), Energy (DOE), State (DOS), Justice (DOJ), and other Federal departments and agencies as appropriate. The Secretary of Homeland Security shall have authority, direction, and control over the DNDO as provided in section 102 (a)(2) of the Homeland Security Act of 2002. The DNDO shall:

(a) Serve as the primary entity in the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device,

fissile material, or radiological material in the United States, and improve that system over time;

(b) Enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(c) Establish, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of Defense and Energy, additional protocols and procedures for use within the United States to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Secretaries of Defense, Homeland Security, and Energy, and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities;

(d) Develop, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of State, Defense, and Energy, an enhanced global nuclear detection architecture with the following implementation:

(i) the DNDO will be responsible for the implementation of the domestic portion of the global architecture;

(ii) the Secretary of Defense will retain responsibility for implementation of DOD requirements within and outside the United States; and

(iii) the Secretaries of State, Defense, and Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with applicable law and relevant international arrangements;

(e) Conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development efforts to support the policy set forth in paragraph (1);

(f) Support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to these entities; and

(g) Further enhance and maintain continuous awareness by analyzing information from all DNDO mission—related detection systems.

(3) To ensure the success of DNDO efforts in support of the policy, the Secretaries of State, Defense, Energy, and Homeland Security, and the Attorney General shall:

(i) determine and provide appropriate nuclear, scientific, and other expertise to the DNDO;

(ii) participate within the DNDO in jointly developing and coordinating detection and response guid-

ance, protocols, and training for Federal. State, local, and tribal officials;

(iii) participate within the DNDO in jointly developing and coordinating the global nuclear detection architecture; and

(iv) where appropriate, participate in the conduct of research and development for nuclear detection.

(4) The Secretary of Energy shall lead the development of nonproliferation research and development and, where appropriate, make available dual-use counter-proliferation and counter-terrorism nuclear detection research and development to DNDO and other entities and officials to support the development of the domestic nuclear and radiological detection system. The Secretary of Energy will make maximum appropriate use of DNDO research, development, test and evaluation programs, and procedures for deploying equipment, taking due account of foreign sensitivities. The Secretary of Energy shall also report information related to detection events to the DNDO. Nothing in this Directive shall be construed to limit or otherwise affect any of the authorities or responsibilities of the Secretary of Energy under any statute, regulation, or executive order.

(5) The Secretary of Defense shall consult with the Secretary of Homeland Security on all aspects of the DNDO to ensure efficiencies, interoperability, and sharing of innovative concepts and operational procedures designed to protect the United States. Nothing in this Directive shall be construed to impair or otherwise affect 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 commanders of the combatant commands, or military command and control procedures.

(6) The Attorney General shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture, particularly as they relate to the development of response guidance protocols and training for Federal, State, local, and tribal law enforcement and information sharing activities. Nothing in this Directive shall be construed to impair or otherwise affect the authority of the Attorney General as stated in Homeland Security Presidential Directive/HSPD-5, "Management of Domestic Incidents," of February 28, 2003.

(7) The Secretary of State shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture, particularly as they relate to overseas detection and reporting activities and to the formulation and implementation of U.S. foreign policy.

(8) The Director of National Intelligence (DNI) shall coordinate with the Secretary of Homeland Security on all aspects of DNDO's global nuclear detection architecture. The DNI also shall ensure the timely dissemination to the DNDO of all radiological, nuclear, and related threats to the United States and other intelligence information relevant to the sup-

port, development, and maintenance of the global nuclear detection architecture and related efforts. Functions assigned by this Directive to the DNI shall be performed by the Director of Central Intelligence until the first DNI is appointed by the President.

(9) This Directive shall be implemented in a manner consistent with applicable law, including the Atomic Energy Act of 1954, the Homeland Security Act of 2002, and the National Security Act of 1947 (all as amended), and presidential guidance, and subject to the availability of appropriations. Nothing in this Directive alters, or impedes the ability to carry out, existing authorities or responsibilities of department and agency heads to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. With regard to nuclear search activities, nothing in this Directive alters in any way existing directives, responsibilities, and roles. 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, entities, officers, employees, or any other person.

(10) Within 120 days after the date of this Directive, and thereafter not less than annually, the Secretary of Homeland Security shall report to me through the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs on the implementation of this Directive, including an assessment of the effectiveness of DNDO and any recommendations for additional enhancements or efforts. The initial implementation report shall include:

(a) the plans for integrated program and budget planning between the appropriate agencies needed to properly execute the DNDO responsibilities and

(b) a joint staffing plan for the DNDO.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—15

[ON THE WAR ON TERRORISM]

MARCH 2006

HSPD—17 is a Classified document and not available for release.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—16

NATIONAL STRATEGY FOR AVIATION SECURITY

MARCH 26, 2007

Prologue

The security and economic prosperity of the United States depend significantly upon the secure operation of its aviation system and use of the world's airspace by the Nation, its international partners, and legitimate commercial interests. Terrorists, criminals, and hostile nation-states have long viewed aviation as a target for attack and exploitation. The tragic events of September 11, 2001 and the Heathrow plot of August 2006 are telling reminders of the threats facing aviation and the intent and capabilities of adversaries that mean to do harm to the United States and its people.

In June 2006, building upon the Administration's successful efforts since 9/11, the President directed the development of a comprehensive National Strategy for Aviation Security (hereafter referred to as "the Strategy") to protect the Nation and its interests from threats in the Air Domain.[1] The Secretary of Homeland Security, in accordance with National Security Presidential Directive-47/Homeland Security Presidential Directive-16 (NSPD-47/HSPD-16), will coordinate the operational implementation of the Strategy, including the integration and synchronization of related Federal programs and initiatives.

Aviation security is best achieved by integrating public and private aviation security global activities into a coordinated effort to detect, deter, prevent, and defeat threats to the Air Domain, reduce vulnerabilities, and minimize the consequences of, and expedite the recovery from, attacks that might occur. The Strategy aligns Federal government aviation security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and tribal governments and the private sector to provide active layered aviation security for, and support defense in-depth of, the United States.

Through a collaborative interagency effort and with input from aviation stakeholders, seven supporting plans will be developed to address the specific threats and challenges identi-

[1] Air Domain is defined as the global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructures.

fied in NSPD-47/HSPD-16. Although the plans will address different aspects of aviation security, they will be mutually linked and reinforce each other. The supporting plans are:

- Aviation Transportation System Security Plan;
- Aviation Operational Threat Response Plan;
- Aviation Transportation System Recovery Plan;
- Air Domain Surveillance and Intelligence Integration Plan;
- International Aviation Threat Reduction Plan;
- Domestic Outreach Plan; and
- International Outreach Plan.

Development of these plans will be guided by the need to revalidate and further enhance current aviation security principles. These plans will be updated on a periodic basis in response to changes in perceived risks to aviation security, the world environment, technology, air transport demands, the global aviation system, and national and homeland security policies. Together, the Strategy and seven supporting plans present a comprehensive national effort to prevent hostile or illegal acts within the Air Domain, promote global economic stability, and protect legitimate aviation activities.

Introduction

"America historically has relied heavily on two vast oceans and two friendly neighbors for border security, and on the private sector for most forms of domestic transportation security. The increasing mobility and destructive potential of modern terrorism has required the United States to rethink and renovate fundamentally its systems for border and transportation security. Indeed, we must now begin to conceive of border security and transportation security as fully integrated requirements because our domestic transportation systems are inextricably intertwined with the global transport infrastructure. Virtually every community in America is connected to the global transportation network by the seaports, airports, highways, pipelines, railroads, and waterways that move people and goods into, within, and out of the Nation. We must therefore promote the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction."

National Strategy for Homeland Security

The United States has a vital national interest in protecting its people, infrastructure, and other interests from threats in the Air Domain. The differences between ground-based and airborne aviation security measures implemented in different jurisdictions throughout the world, the volume of domestic and international air traffic, the speed with which events unfold, and the complexity of aviation assets make the Air Domain uniquely susceptible to attack or exploitation by terrorist groups, hostile nation-states, and criminals.

Adversaries have demonstrated the ability and a continuing desire to exploit vulnerabilities and to adapt to changes in aviation security measures by conducting multiple, simultaneous, catastrophic attacks against the United States and its global interests. Exploitation of the Air Domain by terrorists and hostile nation-

states using unconventional attack methods is not a recent phenomenon. In the 1970s, overseas militant groups hijacked commercial passenger aircraft as a means of garnering international media attention to further their causes. The rise of Islamic religious extremism and state-sponsored terrorism spawned further attacks against civil aviation, including: the hijacking of Trans World Airlines Flight 847 in 1985; the hijacking of Pan Am Flight 73 in 1986 in Karachi, Pakistan; the destruction of Pan Am Flight 103 over Scotland in 1988; and the downing of a French UTA aircraft over Niger in 1989. The attacks of September 11, 2001, brought the reality of these methods to the United States; the Heathrow plot of August 2006 reminds us of the continuing danger.

Over the past five years, the security of the aviation sector has been significantly strengthened through the efforts of the Federal government working with State, local, and tribal governments, the international community, and the private sector. Together these partners continue to implement a broad range of aviation security measures through innovative initiatives and by leveraging pre-existing capabilities to provide the Nation with an active, layered aviation security, and defense in-depth. Such measures include: a federalized Transportation Security Officer workforce that screens passengers and baggage traveling on passenger aircraft; hardened cockpit doors to prevent unauthorized access to the flight deck; Federal Air Marshals who fly anonymously on commercial passenger aircraft to provide a law enforcement presence; enhanced explosives and threat detection technology deployed in hundreds of airports; airspace and air traffic management security measures; and a cadre of canine explosives detection teams screening baggage, cargo, and increasingly, carry-on items.

Other important security activities include: thousands of pilots who voluntarily participate in the Federal Flight Deck Officer program, which permits trained pilots to carry firearms; flight crew members, including flight attendants who have voluntarily taken the Transportation Security Administration's (TSA) Advanced Flight Crew Self-Defense course; other Federal, State, local, and tribal law enforcement officers who travel armed as part of their normal duties; establishment of a program to collect and analyze suspicious events; efforts to streamline operational coordination on incidents both in the air and on the ground; daily vetting of thousands of crew members and passengers on flights to and from the United States; and improvement of surveillance and intelligence sharing. In addition, the Nation's air defense mission has been transformed by expanding surveillance and air interdiction efforts inward to counter terrorist air threats, as well as by continuing traditional air defense activities against the threats from hostile nation-states.

In today's global and interconnected economy, the safe movement of people and cargo across the open skies is a crucial factor in promoting free trade and advancing prosperity and freedom. Defeating the array of threats to the Air Domain requires a common understanding of, and a coordinated effort for, action on a global scale. Nations have a common interest to protect global air travel. Since all nations benefit from this collective security, the United States must encourage all nations to share the responsibility for

maintaining aviation security by countering the threats in this domain.

The Aviation Transportation System[2] comprises a broad spectrum of private and public sector elements, including: aircraft and airport operators; over 19,800 private and public use airports; the aviation sector; and a dynamic system of facilities, equipment, services, and airspace. The Aviation Transportation System continues to grow rapidly, as more and more passengers regularly choose to fly. On a daily basis, thousands of carrier flights arrive, depart, or overfly the continental United States, while each year millions of tons of freight and thousands of tons of mail are transported by air in the United States.

The Nation must be capable of stopping terrorist groups, hostile nation-states, and criminals before they can threaten or engage in attacks against the United States and its international partners, including through the use of weapons of mass destruction (WMD). To achieve these ends, Federal, State, local, and tribal governments and the private sector must take full advantage of strengthened intelligence collection, analysis, and appropriate dissemination; increased sharing of surveillance and other aviation resources; advances in technology; continued enhancements in aviation protective measures; innovations in the use of law enforcement personnel; and strengthened alliances within the public and private sector and other international cooperative arrangements. Military air defense assets are integrated into those activities to provide seamless coverage.

The Strategy does not alter existing authorities or responsibilities of department and agency heads, including their authorities to carry out operational activities or to provide or receive information. It does not change or otherwise affect the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President, to the Secretary of Defense, to the military commanders or military command and control procedures.

Three broad principles provide overarching guidance to the Strategy, its objectives, and its actions. First, the Nation must use the full range of its assets and capabilities to prevent the Air Domain from being exploited by terrorist groups, hostile nation-states, and criminals to commit acts against the United States, its people, its infrastructure, and its other interests. Second, the Nation must ensure the safe and efficient use of the Air Domain. Third, the Nation must continue to facilitate travel and commerce. These guiding principles are critical to global stability and economic growth and are vital to the interests of the United States.

Threats to the Air Domain

Threats to the Air Domain are numerous, complex, and adaptive. While conventional military threats in the Air Domain continue and will likely increase in times of international tension or conflict, the greatest current threat, as demonstrated in the Heathrow plot of August 2006 reminds us of

[2]The Aviation Transportation System is defined as U.S. airspace, all manned and unmanned aircraft operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry.

the continuing danger, and therefore the focus of the Strategy, is terrorism.

Globalization, technological advances, the proliferation of WMD, and the emergence of terrorism as a global phenomenon have enabled threats to the Air Domain to extend in reach, accelerate in speed, and increase in potential impact. Aviation is a global enterprise with a distributed infrastructure and multiple access points. Successful attacks in the Air Domain can inflict mass casualties and grave economic damage, and attract significant public attention because of the impact on the modern transportation system.

Intelligence on threats to the Air Domain plays a critical role in assessing terrorist groups' intentions and capabilities and requires regular update and review to ensure that Federal, State, local, and tribal governments, the private sector, and the international community are taking appropriate measures. However, even the best intelligence will not uncover every specific terrorist plot because of terrorists' efforts at operational secrecy.

Threats focused on the Air Domain can be analyzed in two ways: by originator and by targets and tactics.

Threat Originators

There are three main originators of threats: terrorist groups; hostile nation-states; and other criminals.

Terrorist Groups.

Terrorist groups are politically, as well as religiously in some cases, motivated and use premeditated violence, usually against noncombatants, to affect a particular audience. Because of their clear intent to do harm to the United States and its interests, terrorist groups remain the most severe threat to America's security. Their ultimate goal in the Air Domain is to conduct multiple, simultaneous, catastrophic attacks exploiting the Aviation Transportation System because of its visibility as a symbol of the U.S. global presence and economic influence. In addition, the attacks of September 11, 2001, and other successful or attempted attacks have inspired emulation.

The terrorist threat is changing in form and intensity as terrorists' intentions and capabilities change and countermeasures are instituted. Their techniques are adapting on multiple fronts, including modality of planning, complexity of attack, and style of execution. The type, location, and frequency of terrorist attacks cannot be reliably extrapolated from historical patterns, and therefore current threats must be regularly reassessed.

Terrorist groups, best typified by al-Qa'ida and its affiliates, pose several threats to the Air Domain. The most prominent threat is physical attack, discussed at greater length in the Targets and Tactics section of the Strategy. Terrorists might also take advantage of the same tactics, techniques, and methods pioneered by criminals to counter immigration, customs, and border security measures to move people and materiel. They might deploy in regions of political and economic instability where aviation law enforcement is stretched thin or

readily corruptible, bribe officials, use forged fraudulent documents, and make illegal transactions to hide their true intentions. Terrorists might use unsecured air transportation routes to transport arms, explosives, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists might use these access points and routes to transport more dangerous cargo, including WMD and their associated components. Such threats are particularly worrisome in areas where governments are weak or provide safe haven to terrorists.

Hostile Nation-States.

While most countries have an explicit interest in being able to operate safely, effectively, and reliably in the Air Domain, some pose threats, either due to actual hostile intent or weak infrastructure safeguards. For example, some countries directly sponsor international terrorism, providing training, funding, supplies, WMD and related components, and operational direction to surrogates. Other nation-states knowingly or unknowingly provide safe havens for terrorists who plan, prepare, or facilitate attacks or deploy materiel or operatives through the Air Domain. Some states have weak command and control over their aviation infrastructure, such as their internal air defenses or airport security apparatus, which terrorists can then exploit. Additionally, nation-states could present a military threat, such as cruise missiles, to the United States and U.S. interests globally in the Air Domain.

Criminals

Criminals, including individuals and groups, use the Air Domain to pursue objectives that are illegal under U.S. law or international convention. Domestic extremists in the United States have not, to date, engaged in organized efforts to attack the Aviation Transportation System. However, there are potentially violent domestic groups and individuals who have extensive knowledge of the aviation sector coupled with a demonstrated expertise in manufacturing and employing targeted-attack techniques, including improvised or conventional explosive devices.

Targets and Tactics

There are three primary categories of threats: to and from aircraft; to the Aviation Transportation System infrastructure; and from hostile exploitation of cargo.

Threats to and from Aircraft.

Aircraft can be disaggregated into four categories of threats:

- large passenger aircraft;
- large all-cargo aircraft;
- small aircraft, such as aircraft used primarily to transport small numbers of people or to provide unique services, including light private and corporate aircraft, and helicopters; and

• non-traditional aircraft, such as unmanned aerial vehicles (UAVs), ultra-light aircraft, gliders, and aerial-application aircraft.

These categories might be susceptible to, or could pose a threat from, similar basic tactics: explosives; stand-off weapons including man-portable air defense systems (MANPADS); hijackings; WMD delivery and dissemination; and smuggling of terrorists and instruments of terror.

Large passenger aircraft.

Historically, large passenger aircraft have been at the greatest risk to terrorism because terrorists perceive that such aircraft have great potential to inflict catastrophic damage and are likely to disrupt the Aviation Transportation System. Two tactics have appeared to date. First, aircraft and passengers have been used as targets, such as the detonation of a bomb onboard as was central to the Heathrow plot of 2006, the taking of hostages, traditional hijacking, and attack from stand-off weapons including MANPADS. Second, aircraft have been used as weapons, most notably seen during the September 11, 2001, attacks. The Nation must closely monitor other tactics as they emerge.

Large all-cargo aircraft.

Absent more attractive targets, such as large passenger aircraft, terrorists might seek to take advantage of the varying degrees and sophistication of security measures employed for all-cargo aircraft. If terrorist tactics adapt in this way, large all-cargo aircraft are likely more attractive as weapons, such as through a hijacking to attack ground-based targets or as conveyance mechanisms, rather than as targets. These aircraft also remain at risk from attacks using MANPADS or other stand-off weapons.

Small aircraft.

As with large passenger aircraft, small aircraft face two varieties of threats: as the target of attack; or as weapons used to attack other targets. Small aircraft are relatively unattractive as targets because they carry few passengers, and thus would have less dramatic impact if attacked. As weapons, however, there are several potential threat scenarios. Terrorists might use a wide range of small aircraft, such as business jets or helicopters, to destroy a critical asset or portion of infrastructure. The most serious threat stems from terrorists using small aircraft to transport or deliver WMD or related materiel. The Nation must be especially watchful for terrorists adopting this tactic. Transnational criminal elements employ small aircraft to conduct illicit activities in the Air Domain, including smuggling of persons and contraband.

Non-traditional aircraft.

While ultra-lights, remote-controlled aircraft, gliders, aerial-application aircraft, and UAVs have limited potential as targets, terrorists might employ these non-traditional aircraft as weapons or as a means to disseminate WMD. For example, terrorists might use them for missions that are of limited

range, require limited accuracy, and have a specific and small target. Adoption of this tactic deserves very close monitoring.

While attacks against the Air Domain and the United States and its interests are currently more likely to originate from terrorists, the threat posed by military aircraft of hostile nation-states, such as long range strategic aviation, air-to-air missiles, long-range air-to-surface missiles, or cruise missiles must be considered.

Threats to the Aviation Transportation System Infrastructure.

Reported threats to Aviation Transportation System infrastructure, which comprises airports and those facilities and systems that are used to provide Air Navigation Services (ANS) and other important related services needed to support air operations in U.S. airspace, are relatively few. In part, this is due to the relatively low public profile of ANS infrastructure such as Air Traffic Control facilities and systems, the robustness and resilience of these systems due to many layers of redundancies, and the Nation's likely capacity to recover rapidly and thus limit the psychological or economic impact of any attack.

There is a range of potential threat scenarios at different types of airport facilities that require vigilance. Terrorists might target passenger concentrations at commercial airports, recycling tactics from many years ago. They might place explosives near or inside passenger facilities. Terrorists might target multi-use airports, such as those combining commercial and military operations or commercial and general aviation operations, where unrelated security authorities and dissimilar security procedures often co-exist.

Other Aviation Transportation System-related threats are less likely to materialize. For example, general aviation airports have relatively few passengers in transit and an attack on one would present limited opportunities for causing major symbolic or economic damage. In addition, facilities that process high volumes of cargo have great redundancy and involve few people relative to the commercial passenger aviation system.

Threats from Hostile Exploitation of Cargo.

The air-cargo industry is highly dynamic and encompasses a wide range of users, making it subject to potential exploitation by terrorists. Many users are regulated, from large all-cargo carriers, such as express consignment carriers that operate complex sorting operations at major hubs for time-definite cargo delivery, to small regional carriers, such as those that move high-value cargo or service rural areas. Since the adoption of enhanced security measures at airfreight terminals following September 11, 2001, threats such as stowaways aboard air freighters and the use of explosives for detonation have waned. However, the regulatory framework for cargo systems is not immune to exploitation, especially to methods that have been used by criminals for years. For example, terrorists may infiltrate the cargo handling system to transport people, conventional or WMD, or weapon components.

Risk Methodology

The Strategy will use a risk-based, cross-discipline, and global approach to aviation security to ensure that resources are allocated to those Federal, State, local, and tribal governments and private sector aviation security efforts with the greatest potential to prevent, detect, deter, and defeat attacks, and to mitigate the consequences if an attack occurs. The risk methodology used is outlined in the National Infrastructure Protection Plan (NIPP) and defined in more detail by the NIPP Transportation Sector-Specific Plan (TSSP). These plans define risk as a function of threat, vulnerability, and consequence. The United States Government will regularly conduct formal assessments of the risks to the Aviation Transportation System.

Strategic Objectives

The Strategy describes how the United States Government will enhance the security of the Air Domain while preserving the freedom of the domain for legitimate pursuits. The Strategy recognizes the critical importance of the Air Domain to the United States and the global economy, and is flexible enough to anticipate the dramatic growth in U.S. air traffic and infrastructure as well as emerging threats.

Today's terrorists have demonstrated the capability and intent to inflict a level of damage once reserved exclusively for nation-states. The nations of the world have a shared interest in maintaining and strengthening global aviation security by adopting comprehensive and cohesive policies, programs, and procedures. The Nation reserves its inherent right to self-defense and its right to act to protect its essential national security interests while protecting the United States and its interests. Defending against enemies is a fundamental responsibility of the United States Government.

In keeping with the principles from NSPD-47/HSPD-16, and consistent with the National Strategy for Combating Terrorism, that provide overarching guidance to the Strategy, and in accordance with the values enshrined in the U.S. Constitution and applicable domestic and international law, the following objectives will guide the Nation's aviation security activities:

- deter and prevent terrorist attacks and criminal or hostile acts in the Air Domain;
- protect the United States and its interests in the Air Domain;
- mitigate damage and expedite recovery;
- minimize the impact on the Aviation Transportation System and the U.S. economy; and
- actively engage domestic and international partners.

Deter and Prevent Terrorist Attacks and Criminal or Hostile Acts in the Air Domain

The United States will prevent terrorist attacks and other criminal or hostile acts in the Air Domain by maximizing shared awareness of domestic and international airspace, aviation infrastructure, and those who have access to the system.

International and foreign airspace may also be of national security interest. The United States will work to: detect adversaries before they strike; deny them safe haven in which to operate unobstructed; block their freedom of movement between locations; stop them from entering the United States; identify, disrupt, and dismantle their capacities, including the capacity to possess and access weapons and financial infrastructure; use all means of attribution for maximum legal accountability including criminal prosecution; and take decisive action to eliminate the threat they pose. These actions are addressed in separate executive orders and directives and other presidential guidance.

The basis for effective prevention measures operations and security programs is shared awareness and sharing of risk assessment information, along with credible deterrent and interdiction capabilities. Without effective shared awareness of activities within the Air Domain, crucial opportunities for prevention or an early response can be lost. Advance warning grants time and distance to counter adversaries whether they are planning an operation or are en route to attack or to commit an unlawful act.

Effective prevention requires close cooperation between Federal, State, local, and tribal governments, the private sector, the international community, and the general public to gain shared awareness and increase security in the Air Domain while minimizing the impact of security measures on daily operations. This collaborative effort serves as a force multiplier against adversaries.

Protect the United States and its Interests in the Air Domain

Criminals and terrorists have and will continue to consider the use of the Air Domain as a means to attack the United States. The Nation must therefore continuously monitor, and exert unambiguous control over, its airspace and access to it. Security measures, combined with enhanced surveillance coverage, information collection, shared awareness, dissemination of information, and a ready response capability, will allow the United States to seize the initiative and influence events before adversaries can cause harm.

The security of the United States also depends on the security of the Aviation Transportation System's critical infrastructure, including physical and cyber networks. Complicating the security challenge is the fact that major metropolitan areas within the United States not only have airport and other Aviation Transportation System facilities, but these areas are in close proximity to other critical infrastructure such as military facilities, power plants, refineries, nuclear facilities, chemical plants, tunnels, and bridges.

Maintaining the integrity and viability of the Aviation Transportation System critical infrastructure is essential for the free movement of passengers and goods throughout the world. Some physical and cyber assets, as well as associated infrastructure, also function as defense critical infrastructure, the availability of which must be constantly assured for na-

tional security operations worldwide. Beyond the immediate casualties, the consequences of an attack on a node of critical infrastructure may include disruption of entire systems, significant damage to the economy, or the inability to deploy military forces. Protection of infrastructure networks must address individual elements, interconnecting systems, and their interdependencies.

The Department of Homeland Security is responsible for coordinating the overall national effort to enhance the protection of critical infrastructure. However, public and private sectors must work together to improve national security by: sharing threat information; conducting prudent risk assessments; working to implement essential upgrades; and investing in protective measures such as staff identification and credentialing, access control, and physical security of fixed sites.

Mitigate Damage and Expedite Recovery

The Nation must take actions to mitigate damage and expedite recovery from an attack on the Air Domain. The fundamental key to effective recovery is pre-event planning and established coordination, in conjunction with exercising national mitigation and recovery options. Mitigation and recovery actions promote resilience by preserving life, property, social, economic, and political structures, as well as restoring order and essential services for those who use the Air Domain for their livelihood. However, the Aviation Transportation System will not be shut down as an automatic response to an aviation incident; instead, the United States will be prepared to minimize the impact on the system by isolating particular portions of the Aviation Transportation System, and implementing contingency measures to ensure public safety and continuity of commerce.

The response to incidents will be in accordance with the National Response Plan (NRP), which incorporates the National Incident Management System (NIMS). The NRP provides the structure and mechanisms for national-level policy and operational coordination for domestic incident management. Pursuant to HSPD-5, the Secretary of Homeland Security serves as the principal Federal official for domestic incident management.

A terrorist attack or other disruptive incident involving the Aviation Transportation System can cause severe ripple effects on other modes of transportation as well as adverse economic or national security effects. From the onset of such an incident, Federal, State, local, and tribal governments, along with private sector entities, require the capability to assess the human and economic consequences in affected areas, and to rapidly estimate the effects on other regional, national, or global interests. These entities must also develop and implement contingency procedures to ensure continuity of operations, essential public services, and the resumption or redirection of commercial aviation activities, including the prioritized movement of cargo to mitigate the larger economic, social, and potential national security effects of the incident. For example, the public and private sectors must be ready expeditiously to:

detect and identify potential WMD agents; react without endangering first responders; treat the injured; contain and minimize damage; rapidly reconstitute operations; and mitigate long-term hazards through effective decontamination measures.

Minimize the Impact on the Aviation Transportation System and the U.S. Economy

The Aviation Transportation System demands extremely high standards of security implemented in an efficient manner. Security measures should be balanced with commercial, private, and trade requirements, the safe and efficient movement of cargo and people, and economic and market competition drivers, and should protect privacy and other legal rights. To support the accelerating growth of global commerce and associated U.S. interests, security concerns and measures should, to the extent possible, be: aligned and embedded with business practices; implemented by private sector stakeholders, including air operators and related industries; optimized through the use of information technology; and implemented with the minimum essential impact on commercial and trade-flow costs and operations. The Strategy will require new and enhanced partnerships, as well as cost-sharing and burden-sharing between the public and private sectors.

To accomplish the aforementioned initiatives, the Nation must develop security measures that can be integrated with the unique needs of the aviation sector and provide a high degree of protection, while minimizing the impact to the efficient flow of people and goods through the system. The Nation must depend on new and emerging technologies to assist in this effort, such as the enhancement of biometric solutions for access control initiatives. This effort must also be supported by building and strengthening partnerships between the government and the private sector to: facilitate the continued implementation of security measures; maximize collaborative planning; and coordinate operational responses to incidents.

The effects of response and recovery efforts should also reflect aviation sector needs. On September 11, 2001, the National Airspace System was completely shut down, causing significant operational and economic impacts to the aviation sector. Recognizing the need for diverse and flexible options that allow for an effective response, the United States Government has developed plans allowing for the selective suspension or restriction of air traffic on a local or regional basis as necessary. Plans such as the Emergency Security Control of Air Traffic and other available tools and resources provide government leaders with options for the closure and the reconstitution of the system and include identifying the steps necessary to prevent the recurrence of an event. Efforts such as these will allow the government to continue to provide the security required to protect the Aviation Transportation System while minimizing the impact of those actions on the system and the U.S. economy.

Actively Engage Domestic and International Partners

Effective aviation security includes efforts at home and abroad. Active engagement among Federal, State, local, and tribal governments and private sector stakeholders during the planning process and subsequent follow-up actions is vital for success. Maintaining transparency in the planning effort and promoting dialogue will help increase the effectiveness of risk mitigation actions and reduce burdens on the private sector.

In addition to strengthening relationships among Federal, State, local, and tribal governments, the private sector, and the general public, the Nation must forge cooperative partnerships and alliances with other nations, as well as with public and private stakeholders in the international community. To foster this cooperation, a coordinated policy for United States Government aviation security activities with foreign governments, international and regional organizations, and the private sector must be achieved. Such coordination can help solicit support for improved global aviation security while furthering United States Government policies and goals. Through these domestic and international efforts, the Nation can inculcate common security measures throughout the global aviation community.

Strategic Actions

The differences in ground-based and airborne aviation security measures enacted by the nations of the world, the volume of international air traffic, and the speed of aviation operations make the Air Domain uniquely susceptible to exploitation and disruption by individuals, organizations, and states. Individuals and groups hostile to the United States have demonstrated the ability, and a continuing desire, to exploit vulnerabilities and to adapt to changes in aviation security measures to attack the Nation and its global interests.

The United States recognizes that, because of the extensive global connectivity among businesses, governments, and populations, its aviation security policies affect other nations, and that significant local and regional incidents may have global effects. Success in securing the Air Domain will not come from the United States acting alone, but through a coalition of nations maintaining a strong and united international front. The need for a strong and effective coalition is reinforced by the fact that most of the Air Domain is under no single nation's sovereignty or jurisdiction. Additionally, increased economic interdependency and globalization, made possible by air passenger and cargo transportation, underscore the need for a coordinated international approach. The United States recognizes that the vast majority of actors and activities within the Air Domain are legitimate. The security of the Air Domain can be accomplished only by employing all instruments of national power in a fully coordinated manner in concert with other nation-states.

Aviation security is best achieved by combining public and private aviation security activities on a global scale into a comprehensive and integrated effort that addresses all aviation threats. Aviation security crosses disciplines, builds upon current and future efforts, and depends on scalable, layered security to minimize single points of vulnerability. Full and com-

plete national and international coordination, in concert with cooperative intelligence and information sharing among public and private entities, is required to protect and secure the Air Domain.

The broad principles that provide overarching guidance to the Strategy have been used to direct the development of five strategic actions, which collectively advance the strategic objectives. The Strategy recognizes that collectively these strategic actions support strategic objectives:

- maximize domain awareness;
- deploy layered security;
- promote a safe, efficient, and secure Aviation Transportation System;
- enhance international cooperation; and
- assure continuity of the Aviation Transportation System.

Domain awareness is a critical enabler for all strategic actions. Deploying layered security addresses not only prevention and protection activities, but also the integration of domestic and international security. Clearly, international cooperation is vital to enhancing the effectiveness of each of the other strategic actions.

The Strategy and appropriate supporting plans should ensure bridging toward achieving the Next Generation Air Transportation System (NGATS). NGATS provides an overall and integrated view of future operations beyond the Strategy that will integrate key transformation activities by coordinating applicable policies, procedures, research and development with participating departments and agencies from today's operations into the Aviation Transportation System of 2025.

Maximize Domain Awareness

Maximizing Air Domain awareness is critical to achieving all of the strategic objectives including deterring and preventing terrorist attacks, as well as protecting the United States and its interests in the Air Domain and mitigating the effects of an attack. Achieving shared awareness of the Air Domain is challenging and certain threats to the Air Domain are difficult to detect and interdict. The complexity of aircraft registration and ownership processes, as well as the fluid nature of these activities, offer additional challenges.

To maximize domain awareness the Nation must have the ability to integrate surveillance data, all-source intelligence, law enforcement information, and relevant open-source data from public and private sectors, including international partners. Domain awareness is heavily dependent on advanced information collection, analysis, and sharing of that information, and requires unprecedented cooperation and action among the various elements of the public and private sectors, both nationally and internationally, while adhering to laws protecting U.S. civil liberties. To maximize domain awareness, the United States must leverage the diverse capabilities of the intelligence and law enforcement communities to collect, analyze, integrate, and disseminate timely intelligence to provide a shared awareness for United States Government agencies and international partners.

Additionally, the Nation must refine ongoing efforts to develop shared situational awareness that integrates intelligence, surveillance, reconnaissance, flight, and other aeronautical data, navigation systems, and other operational information. To ensure effective and coordinated action, access to this domain awareness information must be made available at the appropriate classification level to agencies across the U.S. Government, other local government actors, industry partners and the international community. The Nation will continue to enhance the capabilities of current information systems and develop new capabilities and procedures to locate and track aviation threats and illicit activities. Initiatives to maximize domain awareness include:

- The United States Government will maximize its capability to detect and monitor aircraft within its airspace, from large commercial aircraft to low-altitude, low-observable manned or unmanned aircraft, as well as the area contiguous to U.S. airspace and other airspace that might be of national security interest. Priority for surveillance will be given to those assets and those regions identified in specific national level documents.
- The United States Government will enhance its situational awareness through monitoring to include the combination of information sources regarding a flight (for example, airframe characteristic, onboard sensors, crew, passengers, Federal Air Marshals onboard, Federal Flight Deck Officers and domestic and foreign law enforcement).
- The United States Government will develop and encourage regulatory and private sector initiatives to enhance supply chain security practices and advance robust information collection for persons and cargo.
- The United States Government will work with international partners to develop agreements that promote enhanced visibility into the aviation supply chain and the movement of cargo and passengers and will participate in international coalitions to share aviation situational awareness, as protocols permit, on a timely basis.
- The United States Government will continue to improve and invest in an analytic work force, enhanced sensor technology, human intelligence collection, and information processing tools to persistently monitor the Air Domain.
- The United States Government will enhance the global aviation intelligence capability to strengthen intelligence analysis, coordination, and integration.
- The United States Government will enhance the Aviation Transportation System to provide shared situational awareness to disseminate information to both public and private users at the Federal, State, local, and tribal levels.
- The United States Government will support transformational research and development programs in information fusion and analysis to advance to the next level of threat assessment.
- The United States Government, with the cooperation of its foreign partners, will monitor those aircraft, cargo, and

persons of interest from the point of origin, throughout the route of flight, to the point of entry, to ensure the integrity of the transit, to manage aviation traffic routing, and if necessary, to interdict and/ or divert aircraft for law enforcement or defensive action.

Deploy Layered Security

Deploying layered security will be a critical enabler for strategic objectives such as deterring and preventing terrorist attacks, protecting the United States and its interests in the Air Domain, and mitigating damage and expediting recovery. The ability to achieve aviation security is contingent upon an active, layered aviation security and defense in-depth that integrates the capabilities of public and private sector entities acting in concert and using diverse and complementary measures, rather than relying on a single point solution. At a minimum, a layered approach to aviation security means further applying some measure of security to each of the following points: transportation; staff; passengers; conveyances; access control; cargo and baggage; airports; and in-flight security. Together, as one integrated system, these measures allow for resilience against expected and unexpected attack scenarios. Not only does each layer add to security, but its combination serves as a force multiplier. This layered security deters attacks, which otherwise might be executed in a multiple, simultaneous, catastrophic manner, by continually disrupting an adversary's deliberate planning process. The implementation of a new security layer must be cost effective, both in absolute terms and relative to other possible measures, and must protect information privacy and other rights provided by law. Initiatives to enhance layered security include the following:

- The United States Government will further integrate and align all aviation security programs and initiatives into a comprehensive, cohesive national effort of scalable, layered security.
- The United States Government will enhance its capabilities and procedures to identify, intercept, and defeat aviation threats in the air or on the ground.
- The United States Government will expand domestic partnerships with the public and private sector to train and equip domestic security forces, consistent with their jurisdiction and legal authority, to provide physical security for key assets and critical infrastructure to detect, identify, interdict, and defeat aviation threats on the ground.
- The United States Government will conduct and sponsor further development, and where appropriate, encourage implementation of new and emerging technologies including both aircraft-borne and ground-based systems for detection of WMD, as well as for reducing susceptibility/ vulnerability or increasing survivability of aircraft to these and other terrorist threats.
- The United States Government will enhance procedures for identifying and designating flights of interest, as well

as coordinating procedures for any subsequent operational response.

- The United States must have well-trained, properly equipped, and ready ground-based aviation security response forces from State, regional, local, and tribal law enforcement agencies, in addition to a Federal response force ready to detect, deter, interdict, and defeat any potential adversary.
- The United States Government will further collaborate with State, local, and tribal governments and the private sector to assess and prioritize critical facilities, resources, infrastructure, and venues that are at greatest risk from hostile or unlawful acts.
- The United States Government will enhance and expand its capability to assess risks posed by individuals with access to the Air Domain.
- The United States Government, using a risk-based methodology, will continue to develop measures for the prevention and detection of MANPADS or other stand-off weapon attack on domestic commercial aircraft.

Integrating diverse aviation security layers not only requires a clear delineation of roles and responsibilities but also a mutual understanding and acceptance of the supporting nature of overlapping authorities and capabilities of U.S. Government departments and agencies. In particular, to achieve unity of effort and operational effectiveness, aviation security assets must have a high degree of interoperability, reinforced by joint interagency and international training and exercises to ensure a high rate of readiness. Coordination protocols must define procedures for ensuring national execution of aviation security policy for specific threats or incidents.

The integrated planning and management of Federal, State, local, and tribal resources, reinforced with regular exercises, is essential for an effective response. Therefore, agencies will further coordinate training, planning, and other resources, where practical and permissible, to standardize operational concepts, develop common technology requirements, and coordinate budget planning for aviation security missions. Interagency acquisition and logistics processes must support the continuous assessment of all requirements to optimize the allocation of appropriate resources and capabilities. Cooperative research and development efforts, coupled with reformed acquisition processes with coordinated requirements, funding, and scheduling, along with management, will identify current and future needs.

Promote a Safe, Efficient, and Secure Aviation Transportation System

Promoting a safe, efficient, and secure system will help meet the strategic objectives of protecting the United States and its interests in the Air Domain and minimizing the impact on the Aviation Transportation System and the U.S. economy. Potential adversaries will attempt to exploit existing vulnerabilities, choosing the time and place to act according to the weaknesses they perceive. Private owners and operators of

infrastructure, facilities, and resources are the first line of defense and should undertake basic facility security improvements. Defenses against terrorist attacks and criminal acts can be improved by embedding scalable security measures that reduce systemic or physical vulnerabilities. The elimination of vulnerabilities depends upon incorporating best practices and establishing centers of excellence, including feedback mechanisms for lessons learned, and open avenues for internal and external stakeholders to propose and develop security innovations, as well as a periodic review of each country's security standards for mutual compatibility. Initiatives to promote a safe, efficient, and secure Aviation Transportation System include the following:

- The United States Government will assume the function, currently performed by the airlines, of checking passenger information against terrorist watchlist information maintained by the United States Government and vetting such information before the departure of any regularly scheduled commercial flight for which the place of departure, the place of destination, or any scheduled stopping place is within the United States (a "U.S. Flight"). The United States Government will also determine the security utility of performing such function with respect to flights that only pass through U.S. airspace and, if necessary, develop a system by which this function will be performed for such flights.
- The United States Government will continue to collaborate with domestic and international partners to identify options to enhance risk-based screening of passengers, including, the checking of passenger information against terrorist watchlist information for regularly scheduled commercial passenger flights that overfly the territorial airspace of the United States.
- The United States Government, in coordination with public and private partners, will establish requirements for the continued implementation of air cargo transportation security measures, including all-cargo carriers, combination carriers, and indirect air carriers operating to, from, or within the United States.
- The United States Government will develop requirements for the improvement of airspace and air traffic management-related security measures.
- The United States Government and the private sector will continue to conduct vulnerability assessments to identify security measures that require improvement. A consistent risk management approach, which requires a comprehensive assessment of threat, likelihood, vulnerability, and criticality, will allow the private sector to invest in protective measures as a supporting business function.
- The United States Government will encourage the private sector, by means of outcome-based security standards, incentives, and market mechanisms, to conduct comprehensive self-assessments of its supply chain security practices.

- The United States Government will recommend measures to strengthen the prevention of entry by, and detection of, individuals with malicious intent who possess or seek to possess clearance or credentials that permit entry into secure or restricted areas within the Aviation Transportation System.

Enhance International Cooperation

Enhancing international cooperation will be a critical enabler for strategic objectives such as protecting the United States and the Air Domain, actively engaging domestic and international partners, as well as deterring and preventing terrorist attacks and criminal or hostile acts. The United States supports enhancing cooperation among nations and international organizations that share common interests regarding the security of the Air Domain. New initiatives are needed to ensure that all nations fulfill their responsibilities to prevent and respond to terrorist or criminal actions with timely and effective enforcement, including:

- The United States Government will work with foreign partners to enhance international mechanisms to improve transparency in the registration of aircraft, identification of aircraft owners, and transparency of the cargo supply chain.
- The United States Government will further cooperate with foreign partners to enhance and encourage adoption of international standards and best practices as well as to align regulation and enforcement measures. This will include initiatives pursued through international organizations, such as the International Civil Aviation Organization (ICAO), that include industry participation.
- The United States Government will enhance cooperative mechanisms for coordinating international responses to aviation threats that may span national boundaries and jurisdictions.
- The United States will continue to work closely with other governments and international and regional organizations to enhance the aviation security capabilities of other key nations by offering aviation and airport security assistance, training, and consultation.
- The United States Government will promote the implementation of the international anti-air piracy conventions and other international aviation security arrangements and initiatives.

Assure Continuity of the Aviation Transportation System

Assuring the continuity of the Aviation Transportation System will be a critical enabler for strategic objectives such as mitigating damage and expediting recovery, as well as minimizing the impact on the Aviation Transportation System. The United States will be prepared to maintain vital commerce and defense readiness in the aftermath of an attack or other similarly disruptive incident that may occur within the Air Domain. Threats in the Air Domain are dynamic and adaptive; therefore, prevention and protection efforts cannot be relied

upon to prevent all attacks. Resiliency of the Aviation Transportation System and response and recovery efforts are important to minimize the consequences of a disruption within the system and U.S. economy. This requires: a common framework with clearly defined roles for those charged with response and recovery; ready forces that are properly trained and equipped to manage incidents, especially those involving WMD; carefully crafted and exercised contingency plans for response, recovery, and reconstitution; and extensive coordination among public, private, and international communities. Initiatives to assure the continuity of the Aviation Transportation System include:

- The United States Government will develop response and recovery protocols, consistent with the NIMS, to ensure a comprehensive and integrated national effort. Ultimately, these efforts will also need to be aligned with the National Preparedness Goal (NPG), which will establish readiness priorities, targets, and metrics.
- The United States Government will enhance the emergency preparedness for the Aviation Transportation System. This will include pre-staging of resources as necessary, coordinating, and planning exercises with first responders, and planning for restoring the function of the Aviation Transportation System in the event of an incident.
- The United States Government will develop protocols, mechanisms, and processes to mitigate the operational and economic damage from an attack, including the possibility of temporarily suspending or restricting flight operations in select areas of the National Airspace System.
- The United States Government, in coordination with public and private sector partners, will establish near-term and long-term recovery strategies to support the Aviation Transportation System in the event of an attack.
- The United States Government will identify gaps in recovery option capabilities and, working with our State, local, and tribal government, private sector, and international partners, develop appropriate operational and technical solutions to address those gaps.

The direct and indirect costs associated with a prolonged and systemic disruption of the Aviation Transportation System can be significantly reduced by following the provisions of in-place contingency and continuity plans. These plans for assessment, recovery, and reconstitution must prioritize local, regional, and national interests, as well as manage risk and uncertainty within acceptable levels. These contingency and continuity plans must be developed and exercised in a coordinated fashion by the public and private sectors.

Roles and Responsibilities

Because of the complexity and global nature of the Aviation Transportation System, responsibility for preventing, responding to, and, if necessary, recovering from attacks in the Air Domain extends across all levels of government and across private and public sectors. No single entity alone can prevent or mitigate the impact of an attack in the Air Domain. The en-

tities below have roles and responsibilities that fulfill executive orders or statutory responsibilities for Air Domain activities. Given the unique operating environment of the Air Domain, any of these entities may need to perform a specific lead or supporting functional role based on the threat scenario and the outcome desired by the United States Government. In determining whether a specific entity is suitable to perform this role, the following criteria will be considered:

- existing law;
- desired outcome;
- response capabilities required;
- asset availability; and
- authority to act.

To the maximum extent feasible and appropriate, Federal departments and agencies must coordinate their activities with other Federal, State, local, and tribal governments, as well as law enforcement and emergency response agencies.

Department of Homeland Security (DHS)

In accordance with NSPD-47/HSPD-16, the Secretary of Homeland Security is responsible for closely coordinating United States Government activities encompassing the national aviation security programs including identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency solutions. In support of these responsibilities, the Secretary of Homeland Security:

- will conduct regular reviews of national aviation security programs to identify conflicting procedures, identify changes to threats, vulnerabilities, and resulting consequences, and coordinate corresponding interagency mitigation measures;
- will inform Federal government departments when there have been fundamentally significant recommended or actual changes resulting from regular reviews of national aviation security programs;
- will undertake additional initiatives, as appropriate, to maximize aviation security for the United States and its interests;
- is responsible for aviation security law enforcement operations and enforcement and investigation of criminal law violations within the jurisdiction of its law enforcement components;
- is responsible at borders and ports-of-entry for inspection, determining admissibility, and monitoring of persons, conveyances, and cargo traveling via air to ensure compliance with all U.S. laws, including those designed to prevent terrorists, criminals, and terrorist weapons and contraband from entering or exiting the United States; for securing the transport of passengers and cargo by air through domestic and international screening of passengers, baggage, and air cargo; for issuing regulations and security directives necessary to ensure the security of commercial and general aviation aircraft and airport operations; for deployment of law enforcement on U.S. flagged

commercial flights; and for coordination of airport access control and other security measures;

- is responsible for directing law enforcement activity related to the safety of passengers onboard aircraft that are involved in acts of hijackings and air piracy from the moment all external doors of the aircraft are closed following boarding until those doors are opened to allow passengers to leave the aircraft;
- is responsible for collaborating with State, local, and tribal governments and the private sector to assess and prioritize critical facilities, resources, infrastructure, and venues that are at greatest risk from hostile or unlawful acts;
- is responsible for developing technologies to protect assets in the Air Domain against threats such as WMD, MANPADS, and carry-on/ cargo weapons (but not high-end military threats like cruise missiles, which are the purview of the Department of Defense (DoD)), and developing other technologies that facilitate protective measures such as voice and data communications with Federal law enforcement officers;
- is responsible for operational coordination with other United States Government departments and agencies, as well as with foreign governments, in the prevention of and response to aviation security incidents;
- is responsible for advancing common security interests in the Air Domain; and
- is responsible for effecting information sharing related to aviation security in support of an improved global aviation security network.

Department of Transportation (DOT)

The Secretary of Transportation, whose Department includes the country's civil aviation authority and air navigation services provider, is responsible for the regulation and operation of the National Airspace System (NAS). As an integral part of his responsibilities, the Secretary of Transportation is responsible for protecting the nation and U.S. interests in the Air Domain by conducting a broad range of national defense, homeland security, law enforcement, and crisis response related activities, including, but not limited to the following:

- the safe, efficient, and, in cooperation with the Secretaries of Homeland Security and Defense, and other key stakeholders, secure operation of aircraft flying within the country's airspace and that airspace that has been delegated to the United States for the purposes of air navigation services;
- coordinating and managing the air navigation services, regulatory activities, and related functions to support national defense, homeland security, law enforcement, and crisis response missions undertaken by Federal, State, local, and tribal entities, including the imposition of temporary flight restrictions and provision of Air Traffic Control support;

• ensuring the safety of aviation security driven modifications to U.S. registered aircraft and of other aviation security systems, which could affect civil air traffic and the country's air navigation services; the security of the NAS's critical infrastructure, including Air Traffic Control facilities; and

• designated leadership of NGATS/JPDO development, responsible for coordinating of Federal Aviation Administration (FAA), DHS, DoD, National Aeronautics and Space Administration, Department of Commerce, and the Office of Science and Technology Policy participation.

Department of Justice (DOJ)

The Attorney General is responsible for:

• the ground-based tactical response to resolve or defeat a hijacking, air piracy, or other terrorist threat;

• the investigation and prosecution of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States;

• enforcement and investigation of criminal law violations within its jurisdiction that occur in the Air Domain, and all Federal prosecutions arising from these incidents;

• coordinating the activities of other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States; and

• intelligence collection, counterintelligence, and foreign intelligence sharing under guidelines established in statute and policy.

Department of Defense (DoD)

The Secretary of Defense is responsible for:

• deterring, defending against, and defeating aviation threats to the United States and its global interests;

• airborne response and resolution of nation-state threats within the Air Domain;

• the operational response to actual or potential airborne threats in U.S. airspace or the air approaches to the United States, until the threat has either been resolved or defeated;

• taking a lead or supporting role for response to aviation terrorist threats globally as part of the United States Government's active, layered defense of the Nation;

• conducting defense support of civil authorities as directed by the President of the United States or the Secretary of Defense; and

• advising Federal civilian agencies on possible technology development solutions to capability gaps and shall consider collaborative development efforts where appropriate.

DoD is a formally designated partner in NGATS/JPDO initiative through its leadership of the Shared Situational Awareness Integrated Product Team (IPT).

Department of State (DOS)

The Secretary of State is responsible for:

• coordinating United States Government initiatives that involve foreign governments and international organizations, including regional aviation security cooperation;
• visa adjudication;
• giving foreign policy guidance on the U.S. response to actual or potential airborne threats in the air approaches to the United States if those threats are in foreign or international airspace and this is possible in the time available;
• notifying international partners of measures that may affect the exercise of rights under bilateral or multilateral aviation agreements;
• conducting global diplomatic coordination in support of aviation operational threat response, including coordination with foreign states to obtain required authorizations for operations and to facilitate United States Government assistance to operational threat response activities within the jurisdiction of those states, when requested;
• leading operational threat response public affairs activity when it is decided to take an action or refrain from an action based primarily on considerations of foreign policy, and in these cases, the Secretary of State shall also coordinate with other applicable agencies in developing public statements regarding the operational threat response activities and in relaying appropriate press guidance to agencies requesting it;
• evaluating and granting flight clearance into the United States and its territories for foreign military and government-owned aircraft along with any aircraft chartered to transport a cabinet minister or other senior foreign government official, or other official delegation intending to land in, or overfly, the U.S. and its possessions;
• enhancing multilateral nonproliferation controls on MANPADS, and other stand-off weapons systems that pose a threat to civilian and military aviation, and engaging states to seek their adherence to and implementation of those controls;
• implementing MANPADS destruction programs to reduce the global availability of these weapons and provides training and assistance to help states fulfill their MANPADS counter-proliferation obligations and combat illicit arms trade and trafficking within and across their borders; and
• administering and authorizing sanctions that could be applied to governments, entities, or individuals that engage in the proliferation of WMD, MANPADS and other stand-off weapons systems, when those activities meet the statutory and regulatory criteria.

Department of Energy (DOE)

The Secretary of Energy is responsible for:
• providing scientific and technical expertise in nuclear weapons design and specially equipped teams to conduct search, support response, and assist in recovery, and consequence management operations during any radiological or nuclear incident;

• providing radiation detection systems and associated training at foreign border crossings, airports, and seaports to detect and deter illicit trafficking in nuclear and other radioactive materials across international borders; and
• coordinating radiologically contaminated debris management associated with disposition of WMD-related materials and aircraft that may be affected by such materials or attacks.

Department of Commerce (DOC)

The Secretary of Commerce is responsible for:
• providing aviation industry and trade policy expertise in both interagency policy efforts and international negotiations;
• engaging in cooperative efforts on aviation trade issues in numerous international bodies and fora, including ICAO, the Security and Prosperity Partnership (SPP) with Canada and Mexico, the World Trade Organization (WTO), and the Asia Pacific Economic Cooperation (APEC) forum;
• providing analysis of the impact of domestic regulations and international trade agreements on the aviation industry and the broader economy;
• providing the scientific and technical expertise necessary to measure and verify that devices, equipment, and technologies meet or exceed the requirements necessary to maintain and advance the security of the Air Domain;
• providing weather forecast and analysis services integral to the operations of the Aviation Transportation System;
• providing harmonization of U.S. and international standards that are necessary for facilitation of aviation-related commerce; and
• participating in the NGATS initiative through its leadership of the Weather IPT.

Office of The Director of National Intelligence (ODNI)

The Director of National Intelligence is responsible for:
• developing, sustaining, and continually strengthening a unified Intelligence Community enterprise that supports Federal, State, regional, local, tribal, and private sector entities by collecting, analyzing, and disseminating accurate, timely, and relevant all-source intelligence for the safe and effective use of the air, related transportation, and other threat domains;
• defining, creating, and propagating the business rules, policies, and technical standards for an Intelligence Community enterprise environment for information sharing and intelligence integration across the air related transportation, and other threat domains;
• overseeing the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, except intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism; and

- overseeing National Intelligence Program activities that support transportation security, including in the Air Domain, by leveraging innovative collection and analytical techniques, developing and employing effective counterintelligence measures that preserve the integrity of aviation security information, and respecting the civil liberties and privacy of all Americans.

State, Local, and Tribal Governments

Some of the Nation's aviation infrastructure is owned and operated by State, local, and tribal governments. State Governors and/ or homeland security agencies, in addition to local and tribal governments, hold a leadership position to address specific aviation security needs or issues and response. During extraordinary circumstances, the Federal government may assume lead security responsibility. Typically, except for cross-border traffic, lead responsibility will remain with the States, localities, or tribes. Specific responsibilities of State, local, and tribal governments are discussed in the NIPP and corresponding TSSP. State, local, and tribal governments are currently working with the Federal government to identify critical transportation assets, conduct the necessary vulnerability assessments, and develop security plans to protect those assets. They are also developing their response and recovery capabilities to address terrorist attacks and other disruptive incidents, and to meet the NPG.

Private Sector

Substantial segments of the Nation's aviation transportation infrastructure are owned and operated by private sector entities. As such, an effective national aviation security strategy must be supported by a private sector that internalizes a strong security culture, embedding best practices and government requirements into day-to-day operations. It is the responsibility of private sector owners to conduct and execute business continuity planning, integrate security planning with disaster recovery planning, and to actively participate with Federal, State, local, and tribal governments to improve security in the aviation sector.

Conclusion

The Strategy presents a vision for aviation security that seeks to secure the people and interests of the United States. Moreover, it underscores the Nation's commitment to strengthening international partnerships and advancing economic well-being around the globe by facilitating commerce and abiding by the principles of freedom of the airways. The sheer magnitude of the Air Domain complicates the arduous and complex task of maintaining aviation security. The United States confronts a diverse set of adversaries fully prepared to exploit this vast domain for nefarious purposes. The Air Domain serves as the medium for a variety of threats that honor no national frontier and that seek to imperil the peace and prosperity of the world. Many of these threats mingle with legitimate commerce, either to provide concealment for carrying out hostile acts, or to make available weapons of mass destruction, their delivery systems,

and related materials to nations and non-state actors of concern.

In this ambiguous security environment, responding to these unpredictable threats requires teamwork to prevent attacks, protect people and infrastructure, minimize damage, and expedite recovery. The response necessitates the integration and alignment of all aviation security programs and initiatives into a far-reaching and unified national effort involving Federal, State, local, and tribal governments, as well as private sector organizations. Since September 11, 2001, Federal departments and agencies have risen uncompromisingly to the challenge of ensuring aviation security. The challenges that remain ahead for the Nation, the adversaries it confronts, and the environment in which it operates compel the United States to strengthen its ties with international partners and to seek new relationships with others. Therefore, international cooperation is critical to ensuring that lawful private and public activities in the Air Domain are protected from attack and hostile or unlawful exploitation. Such collaboration is fundamental to worldwide economic stability and growth, and it is vital to the interests of the United States. It is only through such an integrated approach among all aviation partners, governmental and non-governmental, public, and private, that the United States can improve the security of the Air Domain.

Thus, effective implementation of the Strategy requires greater cooperation. It requires deeper trust and confidence, not less. It requires a concerted application of collective capabilities to: increase awareness of all people, activities, and events in the Air Domain; enhance aviation security frameworks domestically and internationally through constant innovation; deploy an active, layered aviation security and defense in-depth based on law enforcement authorities, military capabilities, and private sector partners' competencies; pursue transformational research and development to move to the next level of information fusion and analysis and WMD detection technologies for qualitative improvements in threat detection; improve our response posture should a threat emerge; and enhance our recovery should an incident occur.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—17

HSPD—17 is a Classified document and not available for release.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—18

MEDICAL COUNTERMEASURES AGAINST WEAPONS OF MASS DESTRUCTION

JANUARY 31, 2007

BACKGROUND

(1) Weapons of Mass Destruction (WMD) chemical, biological, radiological, and nuclear agents (CBRN) in the possession of hostile states or terrorists represent one of the greatest security challenges facing the United States. An attack utilizing WMD potentially could cause mass casualties, compromise critical infrastructure, adversely affect our economy, and inflict social and psychological damage that could negatively affect the American way of life.

(2) Our National Strategy to Combat Weapons of Mass Destruction (December 2002) and Biodefense for the 21st Century (April 2004) identify response and recovery as key components of our Nation's ability to manage the consequences of a WMD attack. Our primary goal is to prevent such an attack, but we must be fully prepared to respond to and recover from an attack if one occurs. Accordingly, we have made significant investments in our WMD consequence management capabilities in order to mitigate impacts to the public's health, the economy, and our critical infrastructure. The development and acquisition of effective medical countermeasures to mitigate illness, suffering, and death resulting from CBRN agents is central to our consequence management efforts.

(3) It is not presently feasible to develop and stockpile medical countermeasures against every possible threat. The development of vaccines and drugs to prevent or mitigate adverse health effects caused by exposure to biological agents, chemicals, or radiation is a time-consuming and costly process. This directive builds upon the vision and objectives articulated in our National Strategy to Combat Weapons of Mass Destruction and Biodefense for the 21st Century to ensure that our Nation's medical countermeasure research, development, and acquisition efforts:

(a) Target threats that have potential for catastrophic impact on our public health and are subject to medical mitigation;

(b) Yield a rapidly deployable and flexible capability to address both existing and evolving threats;

(c) Are part of an integrated WMD consequence management approach informed by current risk assessments of threats, vulnerabilities, and capabilities; and

(d) Include the development of effective, feasible, and pragmatic concepts of operation for responding to and recovering from an attack.

(4) In order to address the challenges presented by the diverse CBRN threat spectrum, optimize the investments necessary for medical countermeasures development, and ensure that our activities significantly enhance our domestic and international response and recovery capabilities, our decisions as to the research, development, and acquisition of medical countermeasures will be guided by three overarching principles:

(a) Our preparations will focus on countering current and anticipated threat agents that have the greatest potential for use by state and non-state actors to cause catastrophic public health consequences to the American people.

(b) We will invest in medical countermeasures and public health interventions that have the greatest potential to prevent, treat, and mitigate the consequences of WMD threats.

(c) We will link acquisition of medical countermeasures to the existence of effective deployment strategies that are supportable by the present and foreseeable operational and logistic capabilities of Federal, State, and local assets following a WMD attack or other event that presents a catastrophic public health impact.

(5) Mitigating illness and preventing death are the principal goals of our medical countermeasure efforts. As a class, biological agents offer the greatest opportunity for such medical mitigation, and this directive prioritizes our countermeasure efforts accordingly. This directive also provides for tailoring our Nation's ongoing research and acquisition efforts to continue to yield new countermeasures against CBRN agents and for incorporating such new discoveries into our domestic and international response and recovery planning efforts.

Biological Threats

(6) The biological threat spectrum can be framed in four distinct categories, each of which presents unique challenges and significant opportunities for developing medical countermeasures:

(a) Traditional Agents: Traditional agents are naturally occurring microorganisms or toxin products with the potential to be disseminated to cause mass casualties. Examples of traditional agents include Bacillus anthracis (anthrax) and Yersinia pestis (plague).

(b) Enhanced Agents: Enhanced agents are traditional agents that have been modified or selected to enhance their ability to harm human populations or circumvent current countermeasures, such as a bacterium that has been modified to resist antibiotic treatment.

(c) Emerging Agents: Emerging agents are previously unrecognized pathogens that might be naturally occurring and present a serious risk to human populations, such as the virus responsible for Severe Acute Respiratory Syndrome (SARS). Tools to detect and treat these agents might not exist or might not be widely available.

(d) Advanced Agents: Advanced agents are novel pathogens or other materials of biological nature that have been artificially engineered in the laboratory to bypass traditional countermeasures or produce a more severe or otherwise enhanced spectrum of disease.

Nuclear and Radiological Threats

(7) Threats posed by fissile and other radiological material will persist. Our Nation must improve its biodosimetry capabilities and continue to develop medical countermeasures as appropriate to mitigate the health effects of radiation exposure from the following threats:

(a) Improvised Nuclear Devices: Improvised nuclear devices incorporate radioactive materials designed to result in the formation of a nuclear-yield reaction. Such devices can be wholly fabricated or can be created by modifying a nuclear weapon.

(b) Radiological Dispersal Devices: Radiological Dispersal Devices (RDDs) are devices, other than a nuclear explosive device, designed to disseminate radioactive material to cause destruction, damage, or injury.

(c) Intentional Damage or Destruction of a Nuclear Power Plant: Deliberate acts that cause damage to a reactor core and destruction of the containment facility of a nuclear reactor could contaminate a wide geographic area with radioactive material.

Chemical Threats

(8) Existing and new types of chemicals present a range of threats. Development of targeted medical countermeasures might be warranted for materials in the following categories:

(a) Toxic Industrial Materials and Chemicals: Toxic Industrial Materials and Chemicals are toxic substances in solid, liquid, or gaseous form that are used or stored for use for military or commercial purposes.

(b) Traditional Chemical Warfare Agents: Traditional chemical warfare agents encompass the range of blood, blister, choking, and nerve agents historically developed for warfighter use.

(c) Non-traditional Agents: Non-traditional agents (NTAs) are novel chemical threat agents or toxicants requiring adapted countermeasures.

(9) Creating defenses against a finite number of known or anticipated agents is a sound approach for mitigating the most catastrophic CBRN threats; however, we also must simultaneously employ a broad-spectrum "flexible" approach to address other current and future threats. We must be capable of responding to a wide variety of potential challenges, including a novel biological agent that is highly communicable, associ-

ated with a high rate of morbidity or mortality, and without known countermeasure at the time of its discovery. Although significant technological, organizational, and procedural challenges will have to be overcome, such a balanced strategic approach would mitigate current and future CBRN threats and benefit public health.

POLICY

(10) It is the policy of the United States to draw upon the considerable potential of the scientific community in the public and private sectors to address our medical countermeasure requirements relating to CBRN threats. Our Nation will use a two-tiered approach for development and acquisition of medical countermeasures, which will balance the immediate need to provide a capability to mitigate the most catastrophic of the current CBRN threats with long-term requirements to develop more flexible, broader spectrum countermeasures to address future threats. Our approach also will support regulatory decisions and will permit us to address the broadest range of current and future CBRN threats.

Tier I: Focused Development of Agent-Specific Medical Countermeasures

(11) The first tier uses existing, proven approaches for developing medical countermeasures to address challenges posed by select current and anticipated threats, such as traditional CBRN agents. Recognizing that as threats change our countermeasures might become less effective, we will invest in an integrated and multi-layered defense. Department-level strategies and implementation plans will reflect the following three guiding principles and objectives:

(a) Evaluate and clearly define investments in near- and mid-term defenses: We will develop and use risk assessment processes that integrate data and threat assessments from the life science, consequence management, public health, law enforcement, and intelligence communities to guide investment priorities for current and anticipated threats. We will openly identify the high-risk threats that hold potential for catastrophic consequences to civilian populations and warrant development of targeted countermeasures.

(b) Target medical countermeasure strategies to satisfy practical operational requirements: We will model the potential impact of high-risk threats and develop scenario-based concepts of operations for medical consequence management and public health mitigation and treatment of a large-scale attack on our population. These concepts of operations will guide complementary decisions regarding medical countermeasure development and acquisition.

(c) Take advantage of opportunities to buttress U.S. defenses: We will coordinate interagency efforts to identify and evaluate vulnerabilities in our current arsenal of countermeasures to protect the U.S. population. Where appropriate, we will target the development of alternate or supplementary medical countermeasures to ensure that a

multi-layered defense against the most significant high-impact CBRN threats is established.

Tier II: Development of a Flexible Capability for New Medical Countermeasures

(12) Second tier activities will emphasize the need to capitalize upon the development of emerging and future technologies that will enhance our ability to respond flexibly to anticipated, emerging, and future CBRN threats. Importantly, this end-state will foster innovations in medical technologies that will provide broad public health benefit. Department-level strategic and implementation plans will reflect the following guiding principles and objectives:

(a) Integrate fundamental discovery and medical development to realize novel medical countermeasure capabilities: We will target some investments to support the development of broad spectrum approaches to surveillance, diagnostics, prophylactics, and therapeutics that utilize platform technologies. This will require targeted, balanced, and sustained investments between fundamental research to discover new technologies and applied research for technology development to deliver new medical capabilities and countermeasures. Although by no means all-inclusive, our goals could include identification and use of early markers for exposure, greater understanding of host responses to target therapeutics, and development of integrated technologies for rapid production of new countermeasures.

(b) Establish a favorable environment for evaluating new approaches: We must ensure that our investments lead to products that expand the scientific data base, increase the efficiency with which safety and efficacy can be evaluated, and improve the rate at which products under Investigational New Drug or Investigational Device Exemption status progress through the regulatory or approval process. In addition, we must continue to use new tools to evaluate and utilize promising candidates in a time of crisis. Examples of such tools include the "Animal Rule" for testing the efficacy of medical countermeasures against threat agents when human trials are not ethically feasible and the Emergency Use Authorization. Although by no means all-inclusive, our desired end-state could include the use of novel approaches for improved evaluation tools, streamlined clinical trials that meet safety and regulatory needs, and the development and use of novel approaches to manufacturing.

(c) Integrate the products of new and traditional approaches: We must address the challenges that will arise from integrating these new approaches with existing processes. We must incorporate the use of non-pharmacological interventions in our response planning. This integration will forge a flexible biodefense capability that aligns our national requirements for medical countermeasures with the concepts of operation that are used in conjunction with other strategies for mitigating the public health impacts of WMD attacks.

(13) In order to achieve our Tier I and II objectives, it will be necessary to facilitate the development of products and technologies that show promise but are not yet eligible for procurement through BioShield or the Strategic National Stockpile. We will support the advanced development of these products through targeted investments across a broad portfolio, with the understanding that some of these products may be deemed unsuitable for further investment as additional data becomes available, but the expectation that others will become candidates for procurement.

POLICY ACTIONS

(14) We will employ an integrated approach to WMD medical countermeasure development that draws upon the expertise of the public health, life science, defense, homeland security, intelligence, first responder, and law enforcement communities, as well as the private sector, to promote a seamless integration throughout the product development life cycle.

(a) The Secretary of Health and Human Services (Secretary) will lead Federal Government efforts to research, develop, evaluate, and acquire public health emergency medical countermeasures to prevent or mitigate the health effects of CBRN threats facing the U.S. civilian population. The Department of Health and Human Services (HHS) will lead the interagency process and strategic planning and will manage programs supporting medical countermeasures development and acquisition for domestic preparedness.

(i) Stewardship. Not later than 60 days after the date of this directive, the Secretary shall establish an interagency committee to provide advice in setting medical countermeasure requirements and coordinate HHS research, development, and procurement activities. The committee will include representatives designated by the Secretaries of Defense and Homeland Security and the heads of other appropriate executive departments and agencies. This committee will serve as the primary conduit for communication among entities involved in medical countermeasure development. The chair of the committee shall keep the joint Homeland Security Council/National Security Council Biodefense Policy Coordination Committee apprised of HHS efforts to integrate investment strategies and the Federal Government's progress in the development and acquisition of medical countermeasures.

(ii) Strategic Planning. Not later than 60 days after the date of this directive, the Secretary shall establish a dedicated strategic planning activity to integrate risk-based requirements across the threat spectrum and over the full range of research, early-, mid-, and late-stage development, acquisition, deployment, and life-cycle management of medical countermeasures. The Secretary shall align all relevant HHS programs and functions to support this strategic planning.

(iii) Execution. The Secretary shall ensure that the efforts of component agencies, centers and institutes are coordinated and targeted to facilitate both development of near-term medical countermeasures and transformation of our capability to address future challenges. The Secretary shall also establish an advanced development portfolio that targets investments in promising countermeasures and technologies that are beyond early development, but not yet ready for acquisition consideration. In order to realize the full potential for broad partnership with academia and industry, the Secretary shall ensure that HHS coordinates strategies and implementation plans in a manner that conveys integrated priorities, activities, and objectives across the spectrum of relevant Federal participants.

(iv) Engaging the Private Sector and Nongovernmental Entities. The Secretary shall develop and implement a strategy to engage the unique expertise and capabilities of the private sector in developing medical countermeasures to combat WMD, and shall provide clear and timely communication of HHS priorities and objectives. The Secretary shall consider creating an advisory committee composed of leading experts from academia and the biotech and pharmaceutical industries to provide insight on barriers to progress and help identify promising innovations and solutions to problems such as life-cycle management of medical countermeasures. The Secretary shall designate one office within HHS as the principal liaison for nongovernmental entities who wish to bring new technologies, approaches, or potential medical countermeasures to the attention of the Federal Government.

(b) The Secretary of Defense shall retain exclusive responsibility for research, development, acquisition, and deployment of medical countermeasures to prevent or mitigate the health effects of WMD threats and naturally occurring threats to the Armed Forces and shall continue to direct strategic planning for and oversight of programs to support medical countermeasures development and acquisition for our Armed Forces personnel. The Secretaries of Health and Human Services and Defense shall ensure that the efforts of the Department of Defense (DOD) and HHS are coordinated to promote synergy, minimize redundancy, and, to the extent feasible, use common requirements for medical countermeasure development. The Secretary of Defense shall ensure that DOD continues to draw upon its longstanding investment and experience in WMD medical countermeasure research, development, acquisition, and deployment to ensure protection of the Armed Forces, but also to accelerate and improve the overall national effort, consistent with Departmental authorities and responsibilities, and shall ensure that DOD continues to place a special focus on medical countermeasure development for CBRN threat agents because of the unique facilities, testing capabilities, and

trained and experienced personnel within the Department. These efforts will constitute the basis for interagency partnership and combined investment to safeguard the American people.

(c) The Secretary of Homeland Security shall develop a strategic, integrated all-CBRN risk assessment that integrates the findings of the intelligence and law enforcement communities with input from the scientific, medical, and public health communities. Not later than June 1, 2008, the Secretary of Homeland Security shall submit a report to the President through the Assistant to the President for Homeland Security and Counterterrorism, which shall summarize the key findings of this assessment, and shall update those findings when appropriate, but not less frequently than every 2 years. The Department of Homeland Security shall continue to issue Material Threat Determinations for those CBRN agents that pose a material threat to national security.

(d) The Secretaries of Health and Human Services, Defense, and Homeland Security shall ensure the availability of the infrastructure required to test and evaluate medical countermeasures for CBRN threat agents.

(i) The Secretaries of Health and Human Services, Defense, and Veterans Affairs shall leverage their partnership to identify and accelerate research, development, testing, and evaluation programs for the acquisition of medical countermeasures for CBRN threats.

(ii) The Secretary of Health and Human Services and the Secretary of Homeland Security shall develop effective and streamlined processes, including mutually agreed-upon timelines, to assist the respective Secretaries in jointly recommending that the Special Reserve Fund (SRF) be used for the acquisition of specified security countermeasures.

(iii) The Director of National Intelligence shall facilitate coordination across the intelligence community and, in coordination with the Attorney General, engage the law enforcement community to provide all relevant and appropriate WMD-related intelligence information to DHS for the development of the integrated CBRN risk assessment that is used in prioritizing the development, acquisition, and maintenance of medical countermeasures.

GENERAL

(15) This directive:

(a) shall be implemented consistent with applicable law and the authorities of executive departments and agencies, or heads of such departments and agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

GEORGE W. BUSH

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—19

COMBATING TERRORIST USE OF EXPLOSIVES IN THE UNITED STATES

FEBRUARY 12, 2007

Purpose

(1) This directive establishes a national policy, and calls for the development of a national strategy and implementation plan, on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. Definitions

(2) In this directive:

(a) "agencies" means those executive departments enumerated in 5 U.S.C. 101, 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;

(b) "explosive attack" means an act of terrorism in the United States using an explosive;

(c) "explosive" means any chemical compound mixture, or device, the primary or common purpose of which is to function by explosion, including improvised explosive devices, but excluding nuclear and radiological devices;

(d) "improvised explosive device" or "IED" means an explosive device that is fabricated in an improvised manner incorporating explosives or other destructive, lethal, pyrotechnic, or incendiary chemicals;

(e) "NIPP" means the National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive-7 of December 17, 2003 (Critical Infrastructure Identification, Prioritization, and Protection)(HSPD-7); and

(f) "risk" means the product of credible threat, consequence, and vulnerability, as defined in the NIPP. Background

(3) Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide, and there is ample intelligence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosive attacks in the United States is of great concern considering terrorists' ability to make, obtain, and use explosives, the ready availability of components used in IED construction, the

relative technological ease with which an IED can be fashioned, and the nature of our free society. Policy

(4) It is the policy of the United States to counter the threat of explosive attacks aggressively by coordinating Federal, State, local, territorial, and tribal government efforts and collaborating with the owners and operators of critical infrastructure and key resources to deter, prevent, detect, protect against, and respond to explosive attacks, including the following:

(a) applying techniques of psychological and behavioral sciences in the analysis of potential threats of explosive attack;

(b) using the most effective technologies, capabilities, and explosives search procedures, and applications thereof, to detect, locate, and render safe explosives before they detonate or function as part of an explosive attack, including detection of explosive materials and precursor chemicals used to make improvised explosive or incendiary mixtures;

(c) applying all appropriate resources to pre-blast or pre-functioning search and explosives render-safe procedures, and to post-blast or post-functioning investigatory and search activities, in order to detect secondary and tertiary explosives and for the purposes of attribution;

(d) employing effective capabilities, technologies, and methodologies, including blast mitigation techniques, to mitigate or neutralize the physical effects of an explosive attack on human life, critical infrastructure, and key resources; and

(e) clarifying specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery. Implementation Actions

(5) As soon as practicable and not later than 150 days after the effective date of this directive, the Attorney General, in coordination with the Secretary of Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD-7) and agencies that conduct explosive attack detection, prevention, protection, or response activities, shall submit to the President for approval, through the Assistant to the President for Homeland Security and Counterterrorism, a report, including a national strategy and recommendations, on how more effectively to deter, prevent, detect, protect against, and respond to explosive attacks, including the coordination of Federal Government efforts with State, local, territorial, and tribal governments, first responders, and private sector organizations. The report shall include the following:

(a) a descriptive list of all Federal statutes, regulations, policies, and guidance that

(i) set forth agency authorities and responsibilities relating to the prevention or detection of, protection against, or response to explosive attacks, or

(ii) govern the use of the assets and capabilities described in paragraph (b) of this section;

(b) an inventory and description of all current Federal Government assets and capabilities specifically relating to the detection of explosives or the protection against or response to explosive attacks, catalogued by geographic location, including the asset's transportability and, to the extent feasible, similar assets and capabilities of State, local, territorial, and tribal governments;

(c) an inventory and description of current research, development, testing, and evaluation initiatives relating to the detection of and protection against explosives and anticipated advances in capabilities for reducing the threat of explosive attacks, and recommendations for the best means of disseminating the results of such initiatives to and among Federal, State, local, territorial, and tribal governments and first responders, as appropriate;

(d) for the purpose of identifying needed improvements in our homeland security posture, an assessment of our ability to deter, prevent, detect, protect against, and respond to an explosive attack based on a review of risk and the list, inventories, and descriptions developed pursuant to paragraphs (a), (b), and (c) of this section, and recommendations to address any such needed improvements;

(e) recommendations for improved detection of explosive chemical compounds, precursor chemicals used to make improvised explosive chemical compounds, and explosive device components;

(f) recommendations for developing a comprehensive understanding of terrorist training and construction methods relating to explosive attacks and the production of explosive and incendiary materials;

(g) recommendations for protecting critical infrastructure and key resources against an explosive attack that can be used to inform sector-specific plans developed pursuant to the NIPP, including specific actions applicable to each of the critical infrastructure and key resources sectors;

(h) a recommended draft incident annex to the National Response Plan developed pursuant to Homeland Security Presidential Directive-5 of February 28, 2003 (Management of Domestic Incidents), for explosive attacks, detailing specific roles and responsibilities of agencies and heads of agencies through all phases of incident management from prevention and protection through response and recovery;

(i) an assessment of the effectiveness of, and, as necessary, recommendations for improving Federal Government training and education initiatives relating to explosive attack detection, including canine training and performance standards;

(j) recommended components of a national public awareness and vigilance campaign regarding explosive attacks; and

(k) a recommendation on whether any additional Federal Government entity should be established to coordi-

nate Federal Government explosive attack prevention, detection, protection, and response efforts and collaboration with State, local, territorial, and tribal government officials, first responders, and private sector organizations.

(6) Not later than 90 days after the President approves the report, the Attorney General, in coordination with the Secretaries of Defense and Homeland Security and the heads of other Sector-Specific Agencies (as defined in HSPD-7) and agencies that conduct explosive attack detection, prevention, protection, or response activities, shall develop an implementation plan. The implementation plan shall implement the policy set forth in this directive and any recommendations in the report that are approved by the President, and shall include measures to

(a) coordinate the efforts of Federal, State, local, territorial, and tribal government entities to develop related capabilities,

(b) allocate Federal grant funds effectively,

(c) coordinate training and exercise activities, and

(d) incorporate, and strengthen as appropriate, existing plans and procedures to communicate accurate, coordinated, and timely information regarding a potential or actual explosive attack to the public, the media, and the private sector. The implementation plan shall include an implementation timetable, shall be effective upon the approval of the plan by the Attorney General, and shall be implemented by the heads of agencies as specified in the plan. Roles and Responsibilities

(7) The Attorney General, in coordination with the Secretary of Homeland Security and the Director of National Intelligence, shall maintain and make available to Federal, State, local, territorial, and tribal law enforcement entities, and other first responders at the discretion of the Attorney General, a web-based secure portal that includes information on incidents involving the suspected criminal misuse of explosives, including those voluntarily reported by State, local, territorial, and tribal authorities.

(8) The Secretary of Homeland Security, in coordination with the Attorney General, the Director of National Intelligence, and the Secretaries of State and Defense, shall maintain secure information-sharing systems that make available to law enforcement agencies, and other first responders at the discretion of the Secretary of Homeland Security, information, including lessons learned and best practices, concerning the use of explosives as a terrorist weapon and related insurgent war fighting tactics, both domestically and internationally, for use in enhancing the preparedness of Federal, State, local, territorial, and tribal government personnel to deter, prevent, detect, protect against, and respond to explosive attacks in the United States.

(9) The Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Director of the Office of Science and Technology Policy, shall coordinate Federal Government research, development, testing,

and evaluation activities relating to the detection and prevention of, protection against, and response to explosive attacks and the development of explosives render-safe tools and technologies. The heads of all other agencies that conduct such activities shall cooperate with the Secretary of Homeland Security in carrying out such responsibility. General Provisions

(10) This directive:

(a) shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—20

(NATIONAL SECURITY PRESIDENTIAL DIRECTIVE—51)

NATIONAL CONTINUITY POLICY

MAY 4, 2007

Purpose

(1) This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

Definitions

(2) In this directive:

(a) "Category" refers to the categories of executive departments and agencies listed in Annex A to this directive;

(b) "Catastrophic Emergency" means any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions;

(c) "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency;

(d) "Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

(e) "Enduring Constitutional Government," or "ECG," means a cooperative effort among the executive, legisla-

tive, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;

(f) "Executive Departments and Agencies" means the executive departments enumerated in 5 U.S.C. 101, 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;

(g) "Government Functions" means the collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches;

(h) "National Essential Functions," or "NEFs," means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities; and

(i) "Primary Mission Essential Functions," or "PMEFs," means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

Policy

(3) It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions. Implementation Actions

(4) Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

(5) The following NEFs are the foundation for all continuity programs and capabilities and represent the over-

arching responsibilities of the Federal Government to lead and sustain the Nation during a crisis, and therefore sustaining the following NEFs shall be the primary focus of the Federal Government leadership during and in the aftermath of an emergency that adversely affects the performance of Government Functions:

(a) Ensuring the continued functioning of our form of government under Constitution, including the functioning of the three separate branches of government;

(b) Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;

(c) Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests;

(d) Maintaining and fostering effective relationships with foreign nations;

(e) Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests;

(f) Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;

(g) Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and

(h) Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States.

(6) The President shall lead the activities of the Federal Government for ensuring constitutional government. In order to advise and assist the President in that function, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) is hereby designated as the National Continuity Coordinator. The National Continuity Coordinator, in coordination with the Assistant to the President for National Security Affairs (APNSA), without exercising directive authority, shall coordinate the development and implementation of continuity policy for executive departments and agencies. The Continuity Policy Coordination Committee (CPCC), chaired by a Senior Director from the Homeland Security Council staff, designated by the National Continuity Coordinator, shall be the main day-to-day forum for such policy coordination.

(7) For continuity purposes, each executive department and agency is assigned to a category in accordance with the nature and characteristics of its national security roles and responsibilities in support of the Federal Government's ability to sustain the NEFs. The Secretary of Homeland Security shall serve as the President's lead agent for coordinating overall continuity operations and activities of executive departments and

agencies, and in such role shall perform the responsibilities set forth for the Secretary in sections 10 and 16 of this directive.

(8) The National Continuity Coordinator, in consultation with the heads of appropriate executive departments and agencies, will lead the development of a National Continuity Implementation Plan (Plan), which shall include prioritized goals and objectives, a concept of operations, performance metrics by which to measure continuity readiness, procedures for continuity and incident management activities, and clear direction to executive department and agency continuity coordinators, as well as guidance to promote interoperability of Federal Government continuity programs and procedures with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate. The Plan shall be submitted to the President for approval not later than 90 days after the date of this directive.

(9) Recognizing that each branch of the Federal Government is responsible for its own continuity programs, an official designated by the Chief of Staff to the President shall ensure that the executive branch's COOP and COG policies in support of ECG efforts are appropriately coordinated with those of the legislative and judicial branches in order to ensure interoperability and allocate national assets efficiently to maintain a functioning Federal Government.

(10) Federal Government COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority. The Secretary of Homeland Security shall coordinate the integration of Federal continuity plans and operations with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency.

(11) Continuity requirements for the Executive Office of the President (EOP) and executive departments and agencies shall include the following:

(a) The continuation of the performance of PMEFs during any emergency must be for a period up to 30 days or until normal operations can be resumed, and the capability to be fully operational at alternate sites as soon as possible after the occurrence of an emergency, but not later than 12 hours after COOP activation;

(b) Succession orders and pre-planned devolution of authorities that ensure the emergency delegation of authority must be planned and documented in advance in accordance with applicable law;

(c) Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;

(d) Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;

(e) Provision must be made for the availability and redundancy of critical communications capabilities at alternate sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public;

(f) Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and

(g) Provision must be made for the identification, training, and preparedness of personnel capable of relocating to alternate facilities to support the continuation of the performance of PMEFs.

(12) In order to provide a coordinated response to escalating threat levels or actual emergencies, the Continuity of Government Readiness Conditions (COGCON) system establishes executive branch continuity program readiness levels, focusing on possible threats to the National Capital Region. The President will determine and issue the COGCON Level. Executive departments and agencies shall comply with the requirements and assigned responsibilities under the COGCON program. During COOP activation, executive departments and agencies shall report their readiness status to the Secretary of Homeland Security or the Secretary's designee.

(13) The Director of the Office of Management and Budget shall:

(a) Conduct an annual assessment of executive department and agency continuity funding requests and performance data that are submitted by executive departments and agencies as part of the annual budget request process, in order to monitor progress in the implementation of the Plan and the execution of continuity budgets;

(b) In coordination with the National Continuity Coordinator, issue annual continuity planning guidance for the development of continuity budget requests; and

(c) Ensure that heads of executive departments and agencies prioritize budget resources for continuity capabilities, consistent with this directive.

(14) The Director of the Office of Science and Technology Policy shall:

(a) Define and issue minimum requirements for continuity communications for executive departments and agencies, in consultation with the APHS/ CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President;

(b) Establish requirements for, and monitor the development, implementation, and maintenance of, a comprehensive communications architecture to integrate continuity components, in consultation with the APHS/ CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President; and

(c) Review quarterly and annual assessments of continuity communications capabilities, as prepared pursuant to section 16(d) of this directive or otherwise, and report

the results and recommended remedial actions to the National Continuity Coordinator.

(15) An official designated by the Chief of Staff to the President shall:

(a) Advise the President, the Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options; and

(b) Consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.

(16) The Secretary of Homeland Security shall:

(a) Coordinate the implementation, execution, and assessment of continuity operations and activities;

(b) Develop and promulgate Federal Continuity Directives in order to establish continuity planning requirements for executive departments and agencies;

(c) Conduct biennial assessments of individual department and agency continuity capabilities as prescribed by the Plan and report the results to the President through the APHS/CT;

(d) Conduct quarterly and annual assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President;

(e) Develop, lead, and conduct a Federal continuity training and exercise program, which shall be incorporated into the National Exercise Program developed pursuant to Homeland Security Presidential Directive 8 of December 17, 2003 ("National Preparedness"), in consultation with an official designated by the Chief of Staff to the President;

(f) Develop and promulgate continuity planning guidance to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators;

(g) Make available continuity planning and exercise funding, in the form of grants as provided by law, to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators; and

(h) As Executive Agent of the National Communications System, develop, implement, and maintain a comprehensive continuity communications architecture.

(17) The Director of National Intelligence, in coordination with the Attorney General and the Secretary of Homeland Security, shall produce a biennial assessment of the foreign and domestic threats to the Nation's continuity of government.

(18) The Secretary of Defense, in coordination with the Secretary of Homeland Security, shall provide secure, integrated, Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies.

(19) Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall:

(a) Appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency;

(b) Identify and submit to the National Continuity Coordinator the list of PMEFs for the department or agency and develop continuity plans in support of the NEFs and the continuation of essential functions under all conditions;

(c) Plan, program, and budget for continuity capabilities consistent with this directive;

(d) Plan, conduct, and support annual tests and training, in consultation with the Secretary of Homeland Security, in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems; and

(e) Support other continuity requirements, as assigned by category, in accordance with the nature and characteristics of its national security roles and responsibilities

General Provisions

(20) This directive shall be implemented in a manner that is consistent with, and facilitates effective implementation of, provisions of the Constitution concerning succession to the Presidency or the exercise of its powers, and the Presidential Succession Act of 1947 (3 U.S.C. 19), with consultation of the Vice President and, as appropriate, others involved. Heads of executive departments and agencies shall ensure that appropriate support is available to the Vice President and others involved as necessary to be prepared at all times to implement those provisions.

(21) This directive:

(a) Shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) Shall not be construed to impair or otherwise affect

(i) the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals, or

(ii) the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President, to the Secretary of Defense, to the commander of military forces, or military command and control procedures; and

(c) Is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

(22) Revocation. Presidential Decision Directive 67 of October 21, 1998 ("Enduring Constitutional Government and Continuity of Government Operations"), including all Annexes thereto, is hereby revoked.

(23) Annex A and the classified Continuity Annexes, attached hereto, are hereby incorporated into and made a part of this directive.

(24) Security. This directive and the information contained herein shall be protected from unauthorized disclosure, provided that, except for Annex A, the Annexes attached to this directive are classified and shall be accorded appropriate handling, consistent with applicable Executive Orders.

George W. Bush

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE—21

PUBLIC HEALTH AND MEDICAL PREPAREDNESS

OCTOBER 18, 2007

Purpose

(1) This directive establishes a National Strategy for Public Health and Medical Preparedness (Strategy), which builds upon principles set forth in *Biodefense for the 21st Century* (April 2004) and will transform our national approach to protecting the health of the American people against all disasters.

Definitions

(2) In this directive:

(a) The term "biosurveillance" means the process of active data-gathering with appropriate analysis and interpretation of biosphere data that might relate to disease activity and threats to human or animal health — whether infectious, toxic, metabolic, or otherwise, and regardless of intentional or natural origin— in order to achieve early warning of health threats, early detection of health events, and overall situational awareness of disease activity;

(b) The term "catastrophic health event" means any natural or manmade incident, including terrorism, that results in a number of ill or injured persons sufficient to overwhelm the capabilities of immediate local and regional emergency response and health care systems;

(c) The term "epidemiologic surveillance" means the process of actively gathering and analyzing data related to human health and disease in a population in order to obtain early warning of human health events, rapid characterization of human disease events, and overall situational awareness of disease activity in the human population;

(d) The term "medical" means the science and practice of maintenance of health and prevention, diagnosis, treatment, and alleviation of disease or injury and the provision of those services to individuals;

(e) The term "public health" means the science and practice of protecting and improving the overall health of the community through disease prevention and early diagnosis, control of communicable diseases, health education, injury prevention, sanitation, and protection from environmental hazards;

(f) The term "public health and medical preparedness" means the existence of plans, procedures, policies,

training, and equipment necessary to maximize the ability to prevent, respond to, and recover from major events, including efforts that result in the capability to render an appropriate public health and medical response that will mitigate the effects of illness and injury, limit morbidity and mortality to the maximum extent possible, and sustain societal, economic, and political infrastructure; and

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

Background

(3) A catastrophic health event, such as a terrorist attack with a weapon of mass destruction (WMD), a naturally-occurring pandemic, or a calamitous meteorological or geological event, could cause tens or hundreds of thousands of casualties or more, weaken our economy, damage public morale and confidence, and threaten our national security. It is therefore critical that we establish a strategic vision that will enable a level of public health and medical preparedness sufficient to address a range of possible disasters.

(4) The United States has made significant progress in public health and medical preparedness since 2001, but we remain vulnerable to events that threaten the health of large populations. The attacks of September 11 and Hurricane Katrina were the most significant recent disasters faced by the United States, yet casualty numbers were small in comparison to the 1995 Kobe earthquake; the 2003 Bam, Iran, earthquake; the 2004 Sumatra tsunami; and what we would expect from a 1918-like influenza pandemic or large-scale WMD attack. Such events could immediately overwhelm our public health and medical systems.

(5) This Strategy draws key principles from the *National Strategy for Homeland Security* (October 2007), the *National Strategy to Combat Weapons of Mass Destruction* (December 2002), and *Biodefense for the 21st Century* (April 2004) that can be generally applied to public health and medical preparedness. Those key principles are the following: (1) preparedness for all potential catastrophic health events; (2) vertical and horizontal coordination across levels of government, jurisdictions, and disciplines; (3) a regional approach to health preparedness; (4) engagement of the private sector, academia, and other nongovernmental entities in preparedness and response efforts; and (5) the important roles of individuals, families, and communities.

(6) Present public health and medical preparedness plans incorporate the concept of ″surging″ existing medical and public health capabilities in response to an event that threatens a large number of lives. The assumption that conventional public health and medical systems can function effectively in catastrophic health events has, however, proved to be incorrect in real-world situations. Therefore, it is necessary to transform the national approach to health care in the context of a catastrophic health event in order to enable U.S. public health and

medical systems to respond effectively to a broad range of incidents.

(7) The most effective complex service delivery systems result from rigorous end-to-end system design. A critical and formal process by which the functions of public health and medical preparedness and response are designed to integrate all vertical (through all levels of government) and horizontal (across all sectors in communities) components can achieve a much greater capability than we currently have.

(8) The United States has tremendous resources in both public and private sectors that could be used to prepare for and respond to a catastrophic health event. To exploit those resources fully, they must be organized in a rationally designed system that is incorporated into pre-event planning, deployed in a coordinated manner in response to an event, and guided by a constant and timely flow of relevant information during an event. This Strategy establishes principles and objectives to improve our ability to respond comprehensively to catastrophic health events. It also identifies critical antecedent components of this capability and directs the development of an implementation plan that will delineate further specific actions and guide the process to fruition.

(9) This Strategy focuses on human public health and medical systems; it does not address other areas critical to overall public health and medical preparedness, such as animal health systems, food and agriculture defense, global partnerships in public health, health threat intelligence activities, domestic and international biosecurity, and basic and applied research in threat diseases and countermeasures. Efforts in those areas are addressed in other policy documents.

(10) It is not possible to prevent all casualties in catastrophic events, but strategic improvements in our Federal, State, and local planning can prepare our Nation to deliver appropriate care to the largest possible number of people, lessen the impact on limited health care resources, and support the continuity of society and government.

Policy

(11) It is the policy of the United States to plan and enable provision for the public health and medical needs of the American people in the case of a catastrophic health event through continual and timely flow of information during such an event and rapid public health and medical response that marshals all available national capabilities and capacities in a rapid and coordinated manner.

Implementation Actions

(12) *Biodefense for the 21st Century* provides a foundation for the transformation of our catastrophic health event response and preparedness efforts. Although the four pillars of that framework - Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery - were developed to guide our efforts to defend against a bioterrorist attack, they are applicable to a broad array of natural and manmade public health and medical challenges and are

appropriate to serve as the core functions of the Strategy for Public Health and Medical Preparedness.

(13) To accomplish our objectives, we must create a firm foundation for community medical preparedness. We will increase our efforts to inform citizens and empower communities, buttress our public health infrastructure, and explore options to relieve current pressures on our emergency departments and emergency medical systems so that they retain the flexibility to prepare for and respond to events.

(14) Ultimately, the Nation must collectively support and facilitate the establishment of a discipline of disaster health. The specialty of emergency medicine evolved as a result of the recognition of the special considerations in emergency patient care, and similarly the recognition of the unique principles in disaster-related public health and medicine merit the establishment of their own formal discipline. Such a discipline will provide a foundation for doctrine, education, training, and research and will integrate preparedness into the public health and medical communities.

Critical Components of Public Health and Medical Preparedness

(15) Currently, the four most critical components of public health and medical preparedness are biosurveillance, countermeasure distribution, mass casualty care, and community resilience. Although those capabilities do not address all public health and medical preparedness requirements, they currently hold the greatest potential for mitigating illness and death and therefore will receive the highest priority in our public health and medical preparedness efforts. Those capabilities constitute the focus and major objectives of this Strategy.

(16) *Biosurveillance:* The United States must develop a nationwide, robust, and integrated biosurveillance capability, with connections to international disease surveillance systems, in order to provide early warning and ongoing characterization of disease outbreaks in near real-time. Surveillance must use multiple modalities and an in-depth architecture. We must enhance clinician awareness and participation and strengthen laboratory diagnostic capabilities and capacity in order to recognize potential threats as early as possible. Integration of biosurveillance elements and other data (including human health, animal health, agricultural, meteorological, environmental, intelligence, and other data) will provide a comprehensive picture of the health of communities and the associated threat environment for incorporation into the national "common operating picture." A central element of biosurveillance must be an epidemiologic surveillance system to monitor human disease activity across populations. That system must be sufficiently enabled to identify specific disease incidence and prevalence in heterogeneous populations and environments and must possess sufficient flexibility to tailor analyses to new syndromes and emerging diseases. State and local government health officials, public and private sector health care institutions, and practicing clinicians must be involved in system design, and the overall system must be constructed with the principal objective

of establishing or enhancing the capabilities of State and local government entities.

(17) *Countermeasure Stockpiling and Distribution:* In the context of a catastrophic health event, rapid distribution of medical countermeasures (vaccines, drugs, and therapeutics) to a large population requires significant resources within individual communities. Few if any cities are presently able to meet the objective of dispensing countermeasures to their entire population within 48 hours after the decision to do so. Recognizing that State and local government authorities have the primary responsibility to protect their citizens, the Federal Government will create the appropriate framework and policies for sharing information on best practices and mechanisms to address the logistical challenges associated with this requirement. The Federal Government must work with nonfederal stakeholders to create effective templates for countermeasure distribution and dispensing that State and local government authorities can use to build their own capabilities.

(18) *Mass Casualty Care:* The structure and operating principles of our day-to-day public health and medical systems cannot meet the needs created by a catastrophic health event. Collectively, our Nation must develop a disaster medical capability that can immediately re-orient and coordinate existing resources within all sectors to satisfy the needs of the population during a catastrophic health event. Mass casualty care response must be (1) rapid, (2) flexible, (3) scalable, (4) sustainable, (5) exhaustive (drawing upon all national resources), (6) comprehensive (addressing needs from acute to chronic care and including mental health and special needs populations), (7) integrated and coordinated, and (8) appropriate (delivering the correct treatment in the most ethical manner with available capabilities). We must enhance our capability to protect the physical and mental health of survivors; protect responders and health care providers; properly and respectfully dispose of the deceased; ensure continuity of society, economy, and government; and facilitate long-term recovery of affected citizens.

(19) The establishment of a robust disaster health capability requires us to develop an operational concept for the medical response to catastrophic health events that is substantively distinct from and broader than that which guides day-to-day operations. In order to achieve that transformation, the Federal Government will facilitate and provide leadership for key stakeholders to establish the following four foundational elements: Doctrine, System Design, Capacity, and Education and Training. The establishment of those foundational elements must result from efforts within the relevant professional communities and will require many years, but the Federal Government can serve as an important catalyst for this process.

(20) *Community Resilience:* The above components address the supply side of the preparedness function, ultimately providing enhanced services to our citizens. The demand side is of equal importance. Where local civic leaders, citizens, and families are educated regarding threats and are empowered to

mitigate their own risk, where they are practiced in responding to events, where they have social networks to fall back upon, and where they have familiarity with local public health and medical systems, there will be community resilience that will significantly attenuate the requirement for additional assistance. The Federal Government must formulate a comprehensive plan for promoting community public health and medical preparedness to assist State and local authorities in building resilient communities in the face of potential catastrophic health events.

Biosurveillance

(21) The Secretary of Health and Human Services shall establish an operational national epidemiologic surveillance system for human health, with international connectivity where appropriate, that is predicated on State, regional, and community-level capabilities and creates a networked system to allow for two-way information flow between and among Federal, State, and local government public health authorities and clinical health care providers. The system shall build upon existing Federal, State, and local surveillance systems where they exist and shall enable and provide incentive for public health agencies to implement local surveillance systems where they do not exist. To the extent feasible, the system shall be built using electronic health information systems. It shall incorporate flexibility and depth of data necessary to respond to previously unknown or emerging threats to public health and integrate its data into the national biosurveillance common operating picture as appropriate. The system shall protect patient privacy by restricting access to identifying information to the greatest extent possible and only to public health officials with a need to know. The Implementation Plan to be developed pursuant to section 43 of this directive shall specify milestones for this system.

(22) Within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security, shall establish an Epidemiologic Surveillance Federal Advisory Committee, including representatives from State and local government public health authorities and appropriate private sector health care entities, in order to ensure that the Federal Government is meeting the goal of enabling State and local government public health surveillance capabilities.

Countermeasure Stockpiling and Distribution

(23) In accordance with the schedule set forth below, the Secretary of Health and Human Services, in coordination with the Secretary of Homeland Security, shall develop templates, using a variety of tools and including private sector resources when necessary, that provide minimum operational plans to enable communities to distribute and dispense countermeasures to their populations within 48 hours after a decision to do so. The Secretary of Health and Human Services shall ensure that this process utilizes current cooperative programs and engages Federal, State, local government, and private sector entities in template development, modeling, testing, and

evaluation. The Secretary shall also assist State, local government, and regional entities in tailoring templates to fit differing geographic sizes, population densities, and demographics, and other unique or specific local needs. In carrying out such actions, the Secretary shall:

(a) within 270 days after the date of this directive, (i) publish an initial template or templates meeting the requirements above, including basic testing of component distribution mechanisms and modeling of template systems to predict performance in large-scale implementation, (ii) establish standards and performance measures for State and local government countermeasure distribution systems, including demonstration of specific capabilities in tactical exercises in accordance with the National Exercise Program, and (iii) establish a process to gather performance data from State and local participants on a regular basis to assess readiness; and

(b) within 180 days after the completion of the tasks set forth in (a), and with appropriate notice, commence collecting and using performance data and metrics as conditions for future public health preparedness grant funding.

(24) Within 270 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security and the Attorney General, shall develop Federal Government capabilities and plans to complement or supplement State and local government distribution capacity, as appropriate and feasible, if such entities' resources are deemed insufficient to provide access to countermeasures in a timely manner in the event of a catastrophic health event.

(25) The Secretary of Health and Human Services shall ensure that the priority-setting process for the acquisition of medical countermeasures and other critical medical materiel for the Strategic National Stockpile (SNS) is transparent and risk-informed with respect to the scope, quantities, and forms of the various products. Within 180 days after the date of this directive, the Secretary, in coordination with the Secretaries of Defense, Homeland Security, and Veterans Affairs, shall establish a formal mechanism for the annual review of SNS composition and development of recommendations that utilizes input from accepted national risk assessments and threat assessments, national planning scenarios, national modeling resources, and subject matter experts. The results of each such annual review shall be provided to the Director of the Office of Management and Budget and the Assistant to the President for Homeland Security and Counterterrorism at the time of the Department of Health and Human Services' next budget submission.

(26) Within 90 days after the date of this directive, the Secretary of Health and Human Services shall establish a process to share relevant information regarding the contents of the SNS with Federal, State, and local government health officers with appropriate clearances and a need to know.

(27) Within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of State, Defense, Agriculture, Veterans Affairs, and Homeland Security, shall develop protocols for sharing countermeasures and medical goods between the SNS and other Federal stockpiles and shall explore appropriate reciprocal arrangements with foreign and international stockpiles of medical countermeasures to ensure the availability of necessary supplies for use in the United States.

Mass Casualty Care

(28) The Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security, shall directly engage relevant State and local government, academic, professional, and private sector entities and experts to provide feedback on the review of the National Disaster Medical System and national medical surge capacity required by the Pandemic and All-Hazards Preparedness Act (PAHPA) (Public Law 109-417). Within 270 days after the completion of such review, the Secretary shall identify, through a systems-based approach involving expertise from such entities and experts, high-priority gaps in mass casualty care capabilities, and shall submit to the Assistant to the President for Homeland Security and Counterterrorism a concept plan that identifies and coordinates all Federal, State, and local government and private sector public health and medical disaster response resources, and identifies options for addressing critical deficits, in order to achieve the system attributes described in this Strategy.

(29) Within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security, shall:

(a) build upon the analysis of Federal facility use to provide enhanced medical surge capacity in disasters required by section 302 of PAHPA to analyze the use of Federal medical facilities as a foundational element of public health and medical preparedness; and

(b) develop and implement plans and enter into agreements to integrate such facilities more effectively into national and regional education, training, and exercise preparedness activities.

(30) The Secretary of Health and Human Services shall lead an interagency process, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security and the Attorney General, to identify any legal, regulatory, or other barriers to public health and medical preparedness and response from Federal, State, or local government or private sector sources that can be eliminated by appropriate regulatory or legislative action and shall, within 120 days after the date of this directive, submit a report on such barriers to the Assistant to the President for Homeland Security and Counterterrorism.

(31) The impact of the "worried well" in past disasters is well documented, and it is evident that mitigating the mental

health consequences of disasters can facilitate effective response. Recognizing that maintaining and restoring mental health in disasters has not received sufficient attention to date, within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security, shall establish a Federal Advisory Committee for Disaster Mental Health. The committee shall consist of appropriate subject matter experts and, within 180 days after its establishment, shall submit to the Secretary of Health and Human Services recommendations for protecting, preserving, and restoring individual and community mental health in catastrophic health event settings, including pre-event, intra-event, and post-event education, messaging, and interventions.

Community Resilience

(32) The Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Veterans Affairs, and Homeland Security, shall ensure that core public health and medical curricula and training developed pursuant to PAHPA address the needs to improve individual, family, and institutional public health and medical preparedness, enhance private citizen opportunities for contributions to local, regional, and national preparedness and response, and build resilient communities.

(33) Within 270 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Commerce, Labor, Education, Veterans Affairs, and Homeland Security and the Attorney General, shall submit to the President for approval, through the Assistant to the President for Homeland Security and Counterterrorism, a plan to promote comprehensive community medical preparedness.

Risk Awareness

(34) The Secretary of Homeland Security, in coordination with the Secretary of Health and Human Services, shall prepare an unclassified briefing for non-health professionals that clearly outlines the scope of the risks to public health posed by relevant threats and catastrophic health events (including attacks involving weapons of mass destruction), shall coordinate such briefing with the heads of other relevant executive departments and agencies, shall ensure that full use is made of Department of Defense expertise and resources, and shall ensure that all State governors and the mayors and senior county officials from the 50 largest metropolitan statistical areas in the United States receive such briefing, unless specifically declined, within 150 days after the date of this directive.

(35) Within 180 days after the date of this directive, the Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Health and Human Services, and the Director of National Intelligence, shall establish a mechanism by which up-to-date and specific public health threat information shall be relayed, to the greatest extent possible and not inconsistent with the established guidance relating to the Information Sharing Environment, to relevant public

health officials at the State and local government levels and shall initiate a process to ensure that qualified heads of State and local government entities have the opportunity to obtain appropriate security clearances so that they may receive classified threat information when applicable.

Education and Training

(36) Within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretary of Homeland Security, shall develop and thereafter maintain processes for coordinating Federal grant programs for public health and medical preparedness using grant application guidance, investment justifications, reporting, program performance measures, and accountability for future funding in order to promote cross-sector, regional, and capability-based coordination, consistent with section 201 of PAHPA and the National Preparedness Guidelines developed pursuant to Homeland Security Presidential Directive-8 of December 17, 2003 ("National Preparedness").

(37) Within 1 year after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Defense, Transportation, Veterans Affairs, and Homeland Security, and consistent with section 304 of PAHPA, shall develop a mechanism to coordinate public health and medical disaster preparedness and response core curricula and training across executive departments and agencies, to ensure standardization and commonality of knowledge, procedures, and terms of reference within the Federal Government that also can be communicated to State and local government entities, as well as academia and the private sector.

(38) Within 1 year after the date of this directive, the Secretaries of Health and Human Services and Defense, in coordination with the Secretaries of Veterans Affairs and Homeland Security, shall establish an academic Joint Program for Disaster Medicine and Public Health housed at a National Center for Disaster Medicine and Public Health at the Uniformed Services University of the Health Sciences. The Program shall lead Federal efforts to develop and propagate core curricula, training, and research related to medicine and public health in disasters. The Center will be an academic center of excellence in disaster medicine and public health, co-locating education and research in the related specialties of domestic medical preparedness and response, international health, international disaster and humanitarian medical assistance, and military medicine. Department of Health and Human Services and Department of Defense authorities will be used to carry out respective civilian and military missions within this joint program.

Disaster Health System

(39) Within 180 days after the date of this directive, the Secretary of Health and Human Services shall commission the Institute of Medicine to lead a forum engaging Federal, State, and local governments, the private sector, academia, and appropriate professional societies in a process to facilitate the development of national disaster public health and medicine doc-

trine and system design and to develop a strategy for long-term enhancement of disaster public health and medical capacity and the propagation of disaster public health and medicine education and training.

(40) Within 120 days after the date of this directive, the Secretary of Health and Human Services shall submit to the President through the Assistant to the President for Homeland Security and Counterterrorism, and shall commence the implementation of, a plan to use current grant funding programs, private payer incentives, market forces, Center for Medicare and Medicaid Services requirements, and other means to create financial incentives to enhance private sector health care facility preparedness in such a manner as to not increase health care costs.

(41) Within 180 days after the date of this directive, the Secretary of Health and Human Services, in coordination with the Secretaries of Transportation and Homeland Security, shall establish within the Department of Health and Human Services an Office for Emergency Medical Care. Under the direction of the Secretary, such Office shall lead an enterprise to promote and fund research in emergency medicine and trauma health care; promote regional partnerships and more effective emergency medical systems in order to enhance appropriate triage, distribution, and care of routine community patients; promote local, regional, and State emergency medical systems' preparedness for and response to public health events. The Office shall address the full spectrum of issues that have an impact on care in hospital emergency departments, including the entire continuum of patient care from pre-hospital to disposition from emergency or trauma care. The Office shall coordinate with existing executive departments and agencies that perform functions relating to emergency medical systems in order to ensure unified strategy, policy, and implementation.

National Health Security Strategy

(42) The PAHPA requires that the Secretary of Health and Human Services submit in 2009, and quadrennially afterward, a National Health Security Strategy (NHSS) to the Congress. The principles and actions in this directive, and in the Implementation Plan required by section 43, shall be incorporated into the initial NHSS, as appropriate, and shall serve as a foundation for the preparedness goals contained therein.

Task Force and Implementation Plan

(43) In order to facilitate the implementation of the policy outlined in this Strategy, there is established the Public Health and Medical Preparedness Task Force (Task Force). Within 120 days after the date of this directive, the Task Force shall submit to the President for approval, through the Assistant to the President for Homeland Security and Counterterrorism, an Implementation Plan (Plan) for this Strategy, and annually thereafter shall submit to the Assistant to the President for Homeland Security and Counterterrorism a status report on the implementation of the Plan and any recommendations for changes to this Strategy.

(a) The Task Force shall consist exclusively of the following members (or their designees who shall be full-time officers or employees of the members' respective agencies):

(i) The Secretary of Health and Human Services, who shall serve as Chair;

(ii) The Secretary of State;

(ii) The Secretary of Defense;

(iii) The Attorney General;

(iv) The Secretary of Agriculture;

(v) The Secretary of Commerce;

(vi) The Secretary of Labor;

(vii) The Secretary of Transportation;

(viii) The Secretary of Veterans Affairs

(ix) The Secretary of Homeland Security;

(x) The Director of the Office of Management and Budget;

(xi) The Director of National Intelligence; and

(xii) such other officers of the United States as the Chair of the Task Force may designate from time to time.

(b) The Chair of the Task Force shall, as appropriate to deal with particular subject matters, establish subcommittees of the Task Force that shall consist exclusively of members of the Task Force (or their designees under subsection (a) of this section), and such other full-time or permanent part-time officers or employees of the Federal Government as the Chair may designate.

(c) The Plan shall:

(i) provide additional detailed roles and responsibilities of heads of executive departments and agencies relating to and consistent with the Strategy and actions set forth in this directive;

(ii) provide additional guidance on public health and medical directives in Biodefense for the 21st Century; and

(iii) direct the full examination of resource requirements.

(d) The Plan and all Task Force reports shall be developed in coordination with the Biodefense Policy Coordination Committee of the Homeland Security Council and shall then be prepared for consideration by and submitted to the more senior committees of the Homeland Security Council, as deemed appropriate by the Assistant to the President for Homeland Security and Counterterrorism.

General Provisions

(44) This directive:

(a) shall be implemented consistent with applicable law and the authorities of executive departments and agencies, or heads of such departments and agencies, vested by law, and subject to the availability of appropriations and within the current projected spending levels for Federal health entitlement programs;

(b) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(c) is not intended, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

○