

## Homeland Security Presidential Directives (HSPD) Summary

HSPD 1

October 29, 2001  
Amended 2/28/03

### **Organization and Operation of the Homeland Security Council**

Ensures coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.

NSPD-1 is amended under HSPD-5 to include: “The AG, HS Secretary, and Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities.”

HSPD 2

October 29, 2001  
Amended 2/28/03

### **Combating Terrorism Through Immigration Policies**

A. \*National Policy. The United States values immigrants and visitors. Individuals who commit or provide any support for terrorist operations, here or abroad, will be detained, prosecuted, or deported.

1. Foreign Terrorist Tracking Task Force (FTTTF). Attorney General created the FTTTF with Secretary of State, Director of Central Intelligence, and others. Federal agencies must coordinate programs (within law) to deny entry or locate, detain, prosecute or deport aliens involved with terrorism.
  - AG appoints a senior official full time as FTTTF Director who shall report to the Deputy AG, serve as a Senior Advisor to the Assistant to the President for Homeland Security and maintain direct liaison with the Secretary of Homeland Security regarding immigration and foreign terrorists in the US. Director shall consult with Asst. Secretary of State for Consular Affairs on visas.
  - Experts from Secretary of State, DHS, FBI, Secret Service, Customs Service, intelligence community, military support components, and other federal agencies as appropriate to staff the FTTTF mission.
  - AG, HS Secretary and Director of Central Intelligence shall ensure within law that FTTTF requests information from state and local governments.
  - Concurrence of AG, HS Secretary and Director of CI: foreign liaison officers from cooperating countries request expedited investigation and data sharing.
  - Other federal entities: Migrant Smuggling and Trafficking in Persons Coordination Center and Foreign Leads Development Activity shall provide FTTTF with information regarding suspected aliens.
2. Enhanced Department of Homeland Security Capability  
AG and HS Secretary, assisted by Director of Central Intelligence shall immediately develop and implement multi-year plans for investigative and intelligence analysis capabilities of the Department of Homeland Security regarding identifying, locating, detaining, prosecuting or deporting aliens in US involved in or suspected of terrorism. Increases agents (new) assigned to Joint Terrorism Task Forces, as approved by AG and HS Secretary.

3. Abuse of International Student Status

## Homeland Security Presidential Directives (HSPD) Summary

The Secretary of State, HS Secretary and AG, 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 others as deemed needed, shall develop a new program to identify courses and measures to prevent certain international students from receiving education in areas with direct application to the development and use of weapons of mass destruction or for using training to harm the US or its Allies. Department of State, Department of Homeland Security, Department of Justice and US academic institutions shall work together. Includes tracking status of a foreign student with a visa and the source of funds and courses. Guidance shall include control mechanisms like limited duration immigration status or renewal status for students and whether some countries can be exempt.

- Secretary of State, HS Secretary, AG and Secretary of Education shall consult with academic communities and others. The Department of Homeland Security, in consultation with Department of Education, shall conduct periodic reviews to certify compliance of the acceptance of only eligible students.
- 4. North American Complementary Immigration Policies  
Secretary of State, in coordination with Secretary of Homeland Security and AG shall increase sharing, seek shared data-bases across countries and initiate negotiations with Canada and Mexico to assure maximum compatibility of immigration, customs, and visa policies. Maximize assurance and minimize border restrictions for legitimate trans-border commerce.
- 5. Use of Advanced Technologies for Data Sharing and Enforcement Efforts  
Director of Office of Science and Technology Policy (OSTP), in conjunction with the AG, HS Secretary and Director of Central Intelligence, shall make recommendations on advanced technology for enforcement, immigration, rapid identification, of databases for best data mining and to identify any legal barriers to sharing to present to Director of Office of Management and Budget (OMB).
- 6. Budget Support
- 7. OMB shall work with AG, Secretary of State and Treasury, the Assistant to the President for Homeland Security, and other agencies for budget and legislative change to implement.

HSPD 3

March 11, 2002  
Amended 2/28/03

### Homeland Security Advisory System

Assigned to the Secretary of Homeland Security, the HS Advisory System creates a comprehensive, five-level warning system to describe a threat condition with corresponding protective measures to reduce vulnerability or increase response capability that can voluntarily be adopted by state, local, and tribal government and other sectors. The intent is for a common vocabulary, context, and structure for understanding by all government and private citizens.

The nation's risk includes the probability of a terrorist attack and the potential gravity of an occurrence. Except in exigent (difficult or extreme) circumstances, the HS Secretary shall seek the views of the Attorney General and any other appropriate federal agency

## Homeland Security Presidential Directives (HSPD) Summary

heads, including members of the Homeland Security Council on threat conditions. Threat may be for the entire nation or for a particular geographic area or industrial sector. All federal facilities, personnel, and operations inside the territorial US (except military facilities) shall conform with this threat advisory system. At the HS Secretary's request, the Department of Justice shall permit and facilitate the use of delivery systems used or managed for delivering threat advisories. The Director of Central Intelligence, HS Secretary and the AG shall provide the President and select others integrated threat assessments. Details may be shared beyond the federal agencies within the constraints of classification of information; ongoing reviews for sharing will occur, as possible.

Federal departments and agencies are to craft protective measures and have other antiterrorism or self-protection and continuity plans that are resourced, rehearsed, documented, and maintained. Governors, mayors, and leaders of other organizations are encouraged to conduct a similar review as the federal government for an annual assessment.

Threat Condition	Color	Federal (Generic) Protective Measures should be considered:
Low Risk	Green	<ul style="list-style-type: none"> <li>a) refine and exercise preplanned protective measures</li> <li>b) ensure personnel are trained on system of threats and agency-specific or preplanned Protection Actions</li> <li>c) establish a regular assessment process for all facilities and regulated sectors for vulnerability and take reasonable measures to mitigate the vulnerabilities</li> </ul>
Guarded or general risk	Blue	<ul style="list-style-type: none"> <li>d) check communications with designated emergency management response or command locations</li> <li>e) review and update emergency response procedures</li> <li>f) ensure the public is informed and educated to respond appropriately</li> </ul>
Elevated or significant risk	Yellow	<ul style="list-style-type: none"> <li>g) increase surveillance of critical locations</li> <li>h) coordinate emergency plans with nearby jurisdictions, as appropriate</li> <li>i) assess threat characteristics for potential refinement of preplanned protective measures</li> <li>j) implement contingency and emergency response plans, as appropriate</li> </ul>
High risk	Orange	<ul style="list-style-type: none"> <li>k) coordinate necessary security efforts with federal, state, and local (<i>including tribal</i>) law enforcement or any National Guard or other appropriate armed forces organizations</li> </ul>

## Homeland Security Presidential Directives (HSPD) Summary

		<ul style="list-style-type: none"> <li>l) take additional precautions at public events and possibly consider alternative venues or cancellations</li> <li>m) prepare contingency procedures to execute as needed to move to an alternate site or disperse the workforce</li> <li>n) restrict threatened facility access to essential personnel only</li> </ul>
Severe Risk	Red	<p>At this level, it is not anticipated that severe risk protective measures would be sustained for a substantial timeframe.</p> <ul style="list-style-type: none"> <li>o) increase or redirect personnel to address critical emergency needs</li> <li>p) assign emergency response personnel and pre-positioning and mobilizing specially trained teams or resources</li> <li>q) close public and government facilities</li> </ul>

Threat Condition is assigned according to the probability and gravity of risk for a qualitative assessment vs. quantitative calculation. The accuracy is as good as the intel provided. Factors considered include:

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific and/or imminent?
- How grave are the potential consequences of the threat?

HSPD 4  
NSPD 17 Unclassified

September 17, 2001  
December 2002

### **National Strategy to Combat Weapons of Mass Destruction**

Homeland Security will coordinate all federal efforts to prepare for and mitigate the consequences for terrorist attacks within the U.S., per the National Strategy for Homeland Security. The National Security Council's Office of Combating Terrorism coordinates and helps U.S. efforts to respond to and manage the recovery from terrorist attacks outside the U.S., along with the Secretary of State.

Deterrence and taking advantage of today's opportunities, increased emphasis on intelligence collection and analysis, the strengthening of alliance relationships, and the establishment of new partnerships with former adversaries are key to the strategy for national security. As long as there are adversaries that look at weapons of mass destruction beyond a "last resort" option to cause harm to the U.S., our military forces, our friends and allies, the U.S. must be prepared for the unexpected.

The U.S. Military and appropriate **civilian agencies** must be prepared to deter and defend possible WMD employment scenarios with a defense transformation plan to include integrating counter measures in the basic doctrine, training and equipping of all forces to

## Homeland Security Presidential Directives (HSPD) Summary

defeat WMD-armed adversaries. First responders need to be able to respond to chemical, biological, radiological, or nuclear weapons by being trained and equipped with protective, medical and remediation tools to identify, assess, and respond rapidly.

Through diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls will provide deterrents, slow downs or prevention and add to the costs for a terrorist. Ensure compliance of participation in international agreements such as: the Chemical Weapon Convention (CWC); and the Biological Weapons Convention (BWC). Emphasis on strengthening of the Nuclear Nonproliferation Treaty (NPT) and International Atomic Energy Agency (IAEA), including ratification of an IAEA Additional Protocol by all NPT parties with appropriate safeguards and funding. Negotiating a Fissile Material Cut-Off Treaty for U.S. security interests. Strengthen the Nuclear Suppliers Group and Zangger Committee. Effective functioning of the Organization for the Prohibition of Chemical Weapons. Identification and promotion of constructive and realistic measures to strengthen the BWC and help meet the biological weapons threat; and strengthening of the Australia Group. Strengthening the Missile Technology Control Regime (MTCR), including support for universal adherence to the International Code of Conduct Against Ballistic Missile Proliferation. Nunn-Lugar program is followed to reduce the Soviet-WMD and related materials and encourage others to participate through G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction.

Identification and pursuit of new methods of prevention such as national criminalization of proliferation activities and **will look to expand** safety and security measures. The U.S. must be prepared to respond to WMDs and will develop and maintain capability to deter and destroy. The intelligence collection and analysis on WMD, delivery systems and related technologies; research and development to improve response; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists to prevent or eliminate access is an effective avoidance method. Accumulation of plutonium and uranium will be per National Energy Policy and recycling is encouraged. Within a globalized economy, control of certain exports for national security and removal of other barriers to trade through existing and new legislation is necessary. A sanction policy will be developed which may include revising existing policies.

A strong declaratory policy and effective military forces are essential elements of deterrents, including political tools to use against those with or wanting WMD—ensuring it is known that the US will respond with force at home or in support of friends and allies. Air and missile defense along with passive defenses are among the mitigative actions to be taken as well as having back-up plans.

Pillars: Counterproliferation, nonproliferation, and consequence management. Increase intelligence interaction and cooperation among law enforcement and the military, family, friends and allies. Research and development for mitigating WMD consequences or to prioritize, fill gaps and find overlaps for future investment strategies can be shared with the new Counterproliferation Technology Coordination Committee. There are known challenges and organizations, but the strategy can and will succeed.

## Homeland Security Presidential Directives (HSPD) Summary

HSPD 5

February 28, 2003

### Management of Domestic Incidents

The foundation for the 15 exercise scenarios:

- 1) establish a single, comprehensive national incident management system
- 2) Secretary of Homeland Security (4. primary official for domestic incident management to prepare, respond and recover and coordinate federal resources)
  - b) federal departments and agencies are those executive departments enumerated in 5 U.S.C. 101 with DHS and independent establishments defined by 5 U.S.C.104(1); government corporations in 5 U.S.C. 103(1); and US Postal Service.
  - c) state, local, and US geographical same meaning in HSA of 2002, PL 107-296
- 3) policy to prevent, prepare, respond, and recover for terrorist attacks, major disasters and other emergencies (i.e., all hazards). All levels of government to work efficiently and effectively. Crisis management and consequence management are an integrated function.
- 4) HS Secretary is responsible for coordinating federal operations in the US to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

HS Secretary also shall coordinate federal resources used in response to or recovery from terrorist attacks, major disasters, or other emergencies when any one of the following conditions apply:

- a) a federal department or agency, under its own authority, requests assistance of the Secretary.
  - b) resources of state and local authorities are overwhelmed and federal assistance has been requested by the appropriate state or local authorities;
  - c) more than one federal department or agency has become substantially involved in responding to the incident; or
  - d) 4) the HS Secretary has been directed to assume responsibility for managing the domestic incident by the President
- 5) all federal agencies are to cooperate with the Secretary in the domestic incident management role and nothing within the directive changes regular responsibilities of agencies.
- 6) State and local authorities will be assisted by federal government when resources become overwhelmed or federal interests are involved. The HS Secretary will coordinate for state and local governments to have adequate planning, equipment, training, and exercise activities, providing technical assistance to develop all hazards plans and capabilities with prioritized security concerns for ensuring compatibility of all government levels.
- 7) Private and nongovernmental sectors will be coordinated with to promote partnerships and ensure adequate planning, equipment, training, and exercise for incident capabilities.
- 8) Attorney General has lead for criminal investigations and related intelligence collection activities related to terrorist acts or threats. These activities are subject to the National Security Act of 1947 and other applicable law, EO 12333, and Attorney General-approved procedures. FBI, AG, in cooperation with other federal agencies shall coordinate activities among law enforcement to detect, prevent, preempt, and disrupt terrorist attacks against the US. Full capabilities of the US, consistent with law, shall be dedicated to protect national security and assist AG to identify terrorists and bring to

## Homeland Security Presidential Directives (HSPD) Summary

justice. AG and HS Secretary shall establish relationships and mechanisms for cooperation and coordination between their departments.

9) President as Commander in Chief, Secretary of Defense and commanders of military units are not impaired by the directive. Secretary of Defense shall provide military support to civil authorities for domestic incidents when directed or consistent with military readiness. Secretary of Defense retains command of the provision of civil support. Secretaries of Defense and Homeland Security will work out a coordination and cooperation mechanism.

10) Secretary of State has responsibility to protect national security, coordinate international activities of a domestic incident, and protect US citizens and interests abroad.

11) Assistant to the President for Homeland Security and Assistant to the President for National Security Affairs shall be responsible for interagency policy coordination.

12) HS Secretary shall ensure distribution of domestic incidents to all sectors, generally through the Assistant to the President for Homeland Security to the President. Standardized, quantitative reports to the Asst President for Homeland Security on readiness and preparedness of the nation.

13) no authority is added for the Assistant to the President to issue orders.

### Tasking

14) all federal department and agency heads are directed to cooperate, especially in para's 4, 8, 9, and 10.

15) HS Secretary shall develop and submit for review to the HS Council and administer NIMS. System will be consistent nationwide for all government levels, using a core set of concepts, principles, terminology, and technologies for training, identification, resource management, reports, and other methodologies.

16) HS Secretary shall develop, submit to HSC, and administer NRP. Shall consult with Assistants to the President, Economic Policy, Science and Technology, and others to develop the NRP to ensure integration of domestic prevention, preparedness, response, and recovery plans into one all-discipline, all hazards plan. NRP shall be unclassified. If information needs classified, it must be in an annex to the NRP.

a) NRP, using NIMS, shall be used for domestic incidents.

b) NRP will include protocols for operating under different threats and threat levels with integration of federal plans and annexes.

c) NRP will include a consistent report, assessment, and recommendation method.

d) NRP will include direction for improvement to testing, exercising, incident management, and new information and technologies.

17) HS Secretary shall develop initial NRP in 2003, and in consultation with other federal, state, and local governments, develop a national system of standards, guidelines, and protocols to implement NIMS; establish and ensure ongoing management and maintenance of NIMS; and regular consultation among all partners. Review existing authorities and regulations and prepare recommendations to the President on revisions for the final NRP.

18) Heads of federal agencies and departments shall adopt NIMS and NRP (including reports, protocols, maintenance) and provide support and assistance for domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation

## Homeland Security Presidential Directives (HSPD) Summary

activities and support actions of state or local entities.

19) Each federal agency or department head shall revise existing plans with initial NRP in 2003. Submit a plan to adopt and implement NIMS—to be reported to the President.

20) In FY 2005, federal departments and agencies shall require adoption of NIMS, according to law limitations, for preparedness grants, contracts, or other activities, developing standards and guidelines for determining whether a state or local entity has adopted NIMS.

Technical and Conforming Amendments to Homeland Security Presidential Directives  
21) NSPD-1; NSPD-8 (change Office of Homeland Security to the Department of Homeland Security and the Homeland Security Council); HSPD-2; and HSPD-3.

HSPD 6

September 16, 2003

### **Integration and Use of Screening Information**

The policy of the U.S. to protect against terrorism is to 1) develop, integrate, and maintain accurate information about individuals known or suspected of terrorism activity; 2) use the information lawfully, in a manner consistent with the Constitution and rights of all Americans, to support federal, state, local, territorial, tribal, foreign government and private-sector screening processes and diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

Federal agency and executive department heads shall, within law, provide ongoing information to the Terrorist Threat Integration Center (TTIC). The Attorney General, as lead for organization of screening approaches, in coordination with the Secretary of State, HS Secretary, and the Director of Central Intelligence shall implement procedures and safeguards for accessing U.S. citizen's information. The HS Secretary shall develop guidelines for use of the information to support state, local, territorial, and tribal screening processes, and private sector screening when substantially homeland security. The Secretary of State shall develop a proposal for enhancing foreign government cooperation, especially where visa requirements were waived and to establish a screening process of sharing information. No authorities or responsibilities are changed beyond clarifying and improving internal management of federal agencies. See HSPD-11.

HSPD 7

December 17, 2003

### **Critical Infrastructure Identification, Prioritization, and Protection**

Establishes a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources (physical and cyberspace) and to protect these from terrorist attacks. Critical infrastructures and key resources are primarily owned by the private sector and state or local governments. Concerns include catastrophic health effects or mass casualties vs. a weapon of mass destruction, ability to weaken our economy or damage public morale and confidence. This directive is to improve internal management and does not change law or other federal requirements.

Through strategic and tactical enhancements to security, a reduction on impacts or

## Homeland Security Presidential Directives (HSPD) Summary

deterrence of the threat may occur, through establishment of appropriate systems, applicable legal authorities, and presidential guidance. Federal government, state and local governments, and private sector will be informed by HS Secretary of relevant threats to their systems in (28) a “timely manner.”

Definitions: Critical infrastructure see: section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

Key resources: Section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)). Federal departments and agencies in 5 U.S.C. 101, DHS, 5 U.S.C. 104(1); 5 U.S.C. 103(1) and the US Postal Service.

State and local government defined in a geographical sense, section 2 Homeland Security Act of 2002 (6 U.S.C. 101).

Secretary is the Secretary of Homeland Security

Sector-Specific Agency is a federal agency responsible for infrastructure protection activities for designated critical infrastructure sector or key resources.

Protect and secure mean reducing vulnerability of critical infrastructure or key resources to deter, mitigate, or neutralize terrorist attacks.

Avoidance Policy: U.S. to enhance protection of critical infrastructure and key resources that cause catastrophic health effects or mass casualties in comparison to the use of a weapon of mass destruction.

Impair federal agency abilities to perform essential missions or ensure public health and safety.

Undermine government (state and local) capabilities to maintain order and deliver minimum essential public services

Damage private sector’s capability to ensure continuity of economy and delivery of essential services.

Cause economic decline through cascading disruptions of critical facilities and resources  
Undermine public morale and confidence in economy and political institutions.

(8-11) Federal government will identify, prioritize and coordinate protection of critical infrastructure and key resources; protect gathered information; and work to maintain economic stability, all within the law for implementation while working with state and local governments and private sector to avoid catastrophic failure.

(12-17) The HS Secretary shall be responsible for:

coordinating national effort for protection of critical infrastructure and key resources and serve as the principal federal official to lead, integrate, and coordinate implementation among all federal agencies, state and local governments, and the private sector.

Lead for actions 8-11 with particular emphasis for what could be exploited to cause catastrophic health effects or mass casualties comparable to a weapon of mass destruction. Lead for establishing uniform policies, approaches, guidelines, and methodologies within existing federal infrastructure protection and risk management activities across sectors with metrics and criteria for related programs and activities.

HS Secretary shall coordinate protection activities for: information technology, telecommunications, chemical, transportation systems (including mass transit, aviation,

## Homeland Security Presidential Directives (HSPD) Summary

maritime, ground/surface, and rail and pipelines systems); emergency services; and postal and shipping. Coordinate for protection of key resources including dams, government facilities, and commercial facilities. Department shall evaluate need for and coordinate the coverage of additional infrastructure or resource categories. HS Secretary shall facilitate and maintain an organization for security of cyberspace with federal agencies, state and local governments, the private sector, academia and international organizations. Federal agencies will include Departments of Justice, Commerce, Treasury, Defense, Energy, and State, and the CIA to provide analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery for critical infrastructure information systems. This organization will support the Department of Justice and other law enforcement agencies in their missions to investigate and prosecute threats to and attacks against cyberspace, as permitted by law.

(18- Roles:

Department of Agriculture: agriculture, food (meat, poultry, egg products)

Health and Human Services: public health, healthcare, and food (other than meat, poultry, egg products.)

Environmental Protection Agency: drinking water and water treatment

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

Department of Treasury: banking and finance

Department of the Interior: national monuments and icons; and

Department of Defense: defense industrial base

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 federal agencies for convergence and next generation architecture and potential policy change (to provide to the President).

HS Secretary will provide guidance to sector-specific agencies which shall ensure collaboration with other federal agencies, state and local governments and the private sector and key individuals and entities in their infrastructure sector. Conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. Collaboration with all federal agencies, as appropriate, to develop a program, consistent with laws, for geospatial map, image, analyze, and sort critical infrastructure and key resources by using commercial satellite and airborne systems—national technical means should be considered as a last option. HS Secretary with advice from Director of CI, Secretaries of Defense and Interior, and heads of appropriate agencies shall develop mechanisms for mapping program and AG will provide legal advice. The HS Secretary shall use existing and develop new capabilities of agencies to model potential vulnerabilities, placing specific focus on densely populated areas. HS Secretary will develop a national indications and warnings architecture for infrastructure and capabilities that will allow an understanding of baseline operations; identify attack precursors and indicators; and a surge capacity for detecting and analyzing patterns of potential attacks. The architecture shall be coordinated with federal, state, local and non-governmental entities for facilities owned or operated with identification, prioritization,

## Homeland Security Presidential Directives (HSPD) Summary

protection, and contingency planning, including recovery and reconstitution of essential capabilities with an annual plan from federal departments, agencies and sector-specific agencies to be submitted to DHS. All federal agencies are responsible for identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. No authorities are changed, but shall be consistent with legal authorities and presidential guidance.

Implementation: per the Homeland Security Act of 2002: Secretary shall produce comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection with national goals, objectives, milestones, and key initiatives. Also, as appropriate, include a strategy to identify, prioritize, and coordinate protection of critical infrastructure and key resources, such as interactions of all entities including foreign countries and international organizations. Summary of activities necessary to define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources; a summary of initiatives for sharing critical infrastructure and key resources information and how to provide threat warning data to state and local governments and the private sector; and coordination and integration with other emergency management and preparedness activities (NRP, applicable national preparedness goals).

More roles:

Department of State, with DHS and Departments of Justice, Commerce, Defense, the Treasury, and other agencies will work with foreign countries and international organizations to strengthen the protection of US CI/kr.

Department of Justice, including FBI, is tasked to reduce domestic terrorist threats and investigate and prosecute actual or attempted attacks, sabotage or disruptions. AG and HS Secretary shall use cooperation, coordination, current statutory authority and presidential directive(s).

The Department of Commerce, in coordination with HS will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote use of authorities under the Defense Production Act for timely availability of industrial products, materials, and services.

A CI Protection Policy Coordinating Committee will advise HSC on interagency policy and will be chaired by a federal officer or employee designated by the Assistant to the President for Homeland Security.

Office of Science and Technology Policy, in coordination with DHS will coordinate interagency research and development to enhance protection. Nuclear Regulatory Commission and as appropriate, Department of Energy, will be coordinated with HS Secretary for protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and transportation, storage, and disposal of nuclear materials and waste. The HS Secretary, with Director of OSTP shall prepare an annual Federal Research and Development Plan.

OMB shall oversee the implementation of government-wide policies, principles,

## Homeland Security Presidential Directives (HSPD) Summary

standards, and guidelines for federal government computer security programs. The OMB Director will ensure operation of a central federal information security incident center, per Federal Information Security Management Act of 2002.

Per the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving practices for design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of federal agencies.

Department of Transportation and DHS will collaborate on all matters related to transportation security, infrastructure protection, and hazardous materials by all modes (including pipelines) in addition to the national air space system.

Department and sector-specific agencies will collaborate with appropriate private sector and encourage information sharing and analysis mechanisms; collaborate with private sector and support sector-coordinating mechanisms through coordination of protection and sharing of physical and cyber threats.

The HS Secretary, after consulting the HSC, shall designate events as “National Special Security Events” (NSSEs)—this supercedes any past directives and inconsistencies.

This directive supercedes Presidential Decision Directive NSC-63 of 5/22/98 or others that would be inconsistent with HSPD-7.

HSPD 8

December 17, 2003

**National Preparedness** (does not include deter, disrupt, or thwart)

Directs establishment of policies to strengthen all-hazards preparedness capabilities for threatened or actual domestic terrorist attacks, major disasters, and other emergencies.

(3) Companion to HSPD 5 (Management of Domestic Incidents and foundation for the 15 exercise scenarios) for improved response coordination.

(4) Secretary of Homeland Security is the principal federal official for coordinating the implementation of all-hazards preparedness..., to include the support for, and assessment of, the preparedness of state and local first responders.

(5) Develops, in consultation with state and local government, a national preparedness goal, national planning scenarios, universal task list and target capabilities list.

(6) goal will establish measurable readiness priorities and targets to balance the potential threat and magnitude of events.

Focuses on an all-hazard preparedness goal (National Preparedness Goal) for domestic terrorist attacks, major disasters, and other emergencies. The Goal uses capabilities-based planning for catastrophic events with tools such as the 15 planning scenarios, the universal task list, and the target capabilities list. Additionally, there are 7 priorities to include implementing the National Incident Management System and National Response Plan, increase regional collaboration, interoperability communications, strengthen

## Homeland Security Presidential Directives (HSPD) Summary

CBRNE detection, response and decontamination capabilities and strengthen medical surge and mass prophylaxis capabilities.

Issues:

- Federal mandates for funding, yet some jurisdictions will never receive assistance nor potentially be involved.
- Sharing of data. Requiring development of database without specific parameters?
- Timeframes are unreasonable for implementation by all jurisdictions.
- (6) indicates that performance measures will prove capabilities. Does not look at the sustained activities; turn over of staff, and lack of funding.
- (8) indicates there will be a single point of access for federal preparedness assistance within 60 days (of 12/17/03). To be all coordinated, laws in place, applications approved. (e-grants—broke down days prior to final entries for Hazard Mitigation program) (NEMIS—system is down frequently, used for disaster grants)
- Makes terrorism the primary priority for the nation, exclusive of the ongoing hazards faced daily, such as hazardous materials

Washington State SEOO--February 2006

CATEGORY	FEB 2006	FEB 2005	YTD 06	YTD 05
CSEPP INCIDENTS	7	10	9	16
DOE INCIDENTS	0	0	1	1
FIRE	17	15	24	19
HAZMAT	173	158	371	350
OTHER	31	24	52	45
911 OUTAGES	2	4	4	7
SAR	54	35	106	78
TERRORIST	0	0	0	0
WEATHER	5	1	9	5
CGS INCIDENTS	0	1	0	1
ESAR (NOT INCL IN TOTAL)	( 2)	(3)	( 6)	(4)
<b>TOTAL</b>	<b>289</b>	<b>248</b>	<b>576</b>	<b>522</b>

(13) rapid obligation and disbursement of funds has not been fulfilled by the federal governments, yet once the state receives the funds, the clock has started.

(15) equipment purchased requires training, maintenance, and someplace to store, if not additional staff. Many smaller jurisdictions that may need to respond cannot take on this burden.

(17) training and exercise standards. Requires ICS/NIMS, yet “it won’t work for DHS?” Dictating that private industry and others become involved is setting a standard of directing all citizens within state boundaries.

(18) need to look at a worse case scenario for training and exercises and identify joint efforts. Individual hazards may have unique impacts, yet, the state and its partners must be prepared for the daily events, too. Obtaining cooperation among state, local and

## Homeland Security Presidential Directives (HSPD) Summary

private partners is time intensive and expensive.  
(22) private citizens must be integrated. This is a great concept.

HSPD 9

January 30, 2004

### **Defense of United States Agriculture and Food**

Establishes focus and policy to protect agriculture and food systems which are vulnerable to disease, pest, or poisonous agents occurring naturally, unintentionally, or as the result of terrorism while not diminishing the overall economic security. Identify and prioritize sector-critical infrastructure and key resources for protection; develop awareness and early warning capabilities to recognize threats; mitigate vulnerabilities at critical production and processing nodes; enhance screening procedures for domestic and imported products; and enhance response and recovery procedures.

(3) Definitions:

- Critical infrastructure, same meaning as in section 1016(e) USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e))
- Key resources, same meaning as in section 2(9) Homeland Security Act of 2002 (6 U.S.C. 101(9))
- Executive federal departments and agencies, same meaning as in 5 U.S.C. 101 and the Department of Homeland Security; independent agencies, same as in 5 U.S.C. 104(1); government corporations, same as in 5 U.S.C. 103(1); and the United States Postal Service.
- State or local government, in geographical terms, same meaning as in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)
- Sector-Specific agency means a federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Secretary of Homeland Security is Principal Federal Official for implementation for all protection of critical infrastructure and key resources, consistent with HSPD-7.

(7) Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency will perform their responsibilities as Sector-Specific Agencies, as in HSPD-7. Additionally, these agencies, the Secretary of the Interior and other appropriate federal agency heads (¶8) **shall** expand current monitoring and surveillance programs to: increase monitoring systems with international information, animal disease, plant disease, wildlife disease, food, public health, and water quality for providing early detection and awareness of disease, pest, or poisons. Develop systems that track specific animals, plants, commodities and food. Develop nationwide laboratory networks for food, veterinary, plant health, and water quality to integrate federal and state laboratory resources with standard 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 EPA **shall** develop and enhance intelligence operations and analysis capabilities for agriculture, food and water sectors to include

## Homeland Security Presidential Directives (HSPD) Summary

collection and analysis concerning threats, delivery systems, and methods against each sector.

(10) Secretary of Homeland Security **shall** coordinate with Agriculture, Health and Human Services, and EPA, and other federal agency heads appropriate to create a new biological threat awareness capacity to enhance detection and characterization of an attack. Build upon existing surveillance systems (§8) and integrate and analyze domestic and international surveillance and monitoring of data. Recommendations to be published.

(11) Secretaries of Agriculture, HHS, and HS **shall** expand and continue vulnerability assessments for agriculture and food sectors and include requirements of NIPP, updated every 2 years.

(12) HS Secretary and the U.S. Attorney General with Secretary of Ag, HHS, EPA, Dir of CI and other agencies **shall** prioritize, develop and implement mitigation strategies for critical nodes of production or processing to prevent disease, pest and poisonous agents.

(13) Secretary of Ag., HHS, & HS **shall** build on existing or expand development of common screening and inspection procedures for agriculture and foods entering and maximize domestic food inspections.

(14) HS Secretary, in coordination with Secretary of Ag, HHS, AG, and EPA, **will ensure** the combined federal, state and local response capabilities are adequate to be quick and effective to a terrorist attack, major disease outbreak, or other impacts in the national agriculture or food infrastructure and will be integrated with preparedness under HSPD-8.

(15) HS Secretary, in coordination with Secretary of Ag, HHS, AG, and EPA, **shall** develop a coordinated agriculture and food-specific standardized response plan to integrate with the NRP with appropriate roles at government and private sectors and risk communication with the general public.

(16) RPR Secretary of Ag and HHS, in coordination with Secretary HS and EPA **shall** enhance recovery systems for stabilizing agriculture production, food supply, and the economy and rapidly and effectively dispose of infected plants, products, or animals, followed with decontamination.

(17) RPR Secretary of Ag **shall** study and make recommendations to the HSC for use of existing and creating new financial risk management tools to encourage self-protection for agriculture and food enterprises vulnerable to terrorism impacts.

(18) RPR Secretary of Ag in coordination with Secretary of HS and consultation HHS and EPA shall work with state and local governments and private sectors to develop:

a) National Veterinary Stockpile (NVS) to contain animal vaccine, antiviral, or therapeutic products to respond to the most damaging animal diseases affecting human health and the economy; available within 24 hours. Leverage mechanisms and infrastructure for management, storage, and distribution of the Strategic National Stockpile with NVS.

b) National Plant Disease Recovery System (NPDRS) to provide pest control measures and resistant seed varieties capable of producing economic crops within a single growing season. Emergency planning shall provide for 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.

(19) O&PD Secretary of HS, in coordination with the Secretaries of Ag, HHS, and heads of other federal departments and agencies, shall work with private sectors to establish

## Homeland Security Presidential Directives (HSPD) Summary

information sharing and analysis mechanisms for agriculture and food.

(20) O&PD Secretary of Ag and HHS, in consultation with Secretaries of HS and Ed, shall support development of and promote a higher ed program for food (animal, plant, and public health) supply protection. May fund training in exotic animal diseases, other.

(21) O&PD Secretary of Ag and HHS, in consultation with Secretaries of HS and Ed, shall support higher ed training for food defense professionals to protect food supply.

(22) O&PD Secretary of Ag, HHS and HS shall establish professional development and training opportunities in agriculture and food protection, such as intern/fellowships.

(23) R&D Secretary of HS (lead coordination) with Ag, and HHS, EPA, and heads of other federal departments and agencies, in consultation with the Director of the Office of Science and Technology Policy, prioritize research and development of countermeasures, current and new, against intentional introduction of animal, plant or zoonotic diseases to include detection, prevention, agent characterization, and dose responses.

(24) R&D Secretary of Ag and HS will develop a plan for agricultural biocontainment labs to diagnosis foreign animal and zoonotic diseases.

(25) R&D Secretary of HS, in consultation with Sec of Ag and HHS, **shall** establish university-based centers of excellence in agriculture and food security.

(26) B Secretary of Ag, HHS and HS shall submit concurrent budget submissions for an integrated food system defense budget plan.

(27) I. Nothing is altered in the current authorities of federal departments and agencies by this directive.

(28) I. Intent is for improvement of internal management of federal executive branch and creates no changes to rights or benefits.

HSPD 10

April 28, 2004

### **Biodefense for the 21st Century**

Biological weapons attacks could cause catastrophic harm, widespread injury and result in massive casualties and economic disruption. Biological attacks can mimic naturally-occurring disease which can delay recognition and uncertainty of an event allowing the attacker to escape due to delays. Disease outbreaks respect no geopolitical boundaries which means an attack can occur outside the US and be spread through contagious individuals. Prevention, detection, control, and treatment will be challenging as biotechnology and science expertise advances and can be no notice events and adversaries look for opportunities to cause catastrophic numbers of acute casualties, long-term disease and disability, psychological trauma and mass panic; disrupt critical sectors of our economy and day-to-day lives of Americans' and create cascading international effects by disrupting and damaging international trade relationships—here or abroad.

The US has a strong biomedical research infrastructure and has expanded international research relations. Medical and public health infrastructure is being expanded (although not all labs are linked yet). As of 2004, the US has:

- expanded international efforts to keep biological materials away from terrorists
- launched the proliferation Security Initiative to prevent biological and weapons of mass destruction
- established Biowatch program—network of environmental sensors to detect

## Homeland Security Presidential Directives (HSPD) Summary

- biological weapons attacks in major cities
- new programs initiated to secure and defend agriculture and food systems against biological contamination
- Increased DHHS bioterrorism research funding by 30%
- Expanded the Strategic National Stockpile of medicines for treating victims of bioterror attacks, ensuring push packages can be anywhere in the US within 12 hours
- Stockpiles were created for smallpox vaccine for every American and vaccinated over 450,000 armed service members
- Launched and funded Project Bioshield to speed 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 of attacks
- Worked with the international community to strengthen global, regional and national programs to prevent, detect, and respond to attacks
- Conducted a comprehensive, self-assessment for identifying future biological defense priorities and supporting actions. The results are the blueprint for Biodefense for the 21<sup>st</sup> Century that integrates a sustained effort for national and homeland security, medical, public health, intelligence, diplomatic, and law enforcement communities. Specific instructions are in a classified version of this document.

Integrating federal policy, coordination, and planning with the capabilities of federal, state and local government and private sector levels, in addition to close international cooperation with friends and allies to maximize prevention, protection and mitigation of biological weapons attacks. Continuing the quick protection for constantly changing threats (for multiple or repetitive attacks) to the public health and medical systems, care providers and public health officials remain the first line of defense. “Private, local and state capabilities are being augmented by and coordinated with federal assets.”

The focus for agriculture, food and water protection remains on natural or unintentional disease introduction and to anticipate potential threats. Enhanced security, medical protection, and training for the military for these threats, allows the US to operate effectively.

### Pillars of Biodefense:

HS Secretary is principal federal official for domestic incident management and coordination of domestic federal operations and most resources to prepare for, respond to, and recover from biological weapons attacks.

Secretary of State is principle federal officer for international terrorist incidents that occur outside the US Territory, including US support for foreign consequence management (as approved by DOD) and coordinates with appropriate federal agencies.

### **Threat awareness**

\*Biological Warfare Related Intelligence: Improve intelligence community’s ability to collect, analyze and disseminate through increased, dedicated resources and an aggressive approach to look at forward analyses, include Red Teams and scientific methods for placing or developing intelligence collection and sensing.

## **Homeland Security Presidential Directives (HSPD) Summary**

\*Assessments: Periodic assessments of the evolving biological threats and capabilities to effectively research, develop, plan and prepare or respond to prioritized threats. A periodic senior-level policy net assessment for measuring implementation, gaps, or vulnerabilities and make recommendations for refocus of resources; HS Secretary is responsible for working with other federal agencies in conducting the assessments.

\*DHHS is coordination with other federal agencies is working towards an integrated and focused national effort to anticipate and respond to emerging threats. Strengthen medical, public health, agricultural, defense, law enforcement, diplomatic, environmental, and transportation infrastructures to recognize, confront and contain impact of threats.

### **Prevention and Protection**

Preventing a biological weapons attack is less costly than responding and recovery from an attack. Diplomacy, arms control, law enforcement, multilateral export controls and threat reduction assistance are being enhanced. International coalitions are supporting these efforts. The National Strategy to Combat Weapons of Mass Destruction, 12/02, places emphasis on proactive steps for which the US will continue to detect and destroy assets through the Proliferation Security Initiative. Departments of State, Defense, Justice and the Intelligence Community have vital roles for proactive prevention.

\*Critical Infrastructure Protection from biological weapons is a priority as there may be access denied for essential facilities and response capabilities. Survivability, continuity and restoration of operations. Priority sectors are medical, public health, food, water, energy, agricultural and transportation sectors with DHS working with federal agencies on biodetection technologies and decontamination methodologies.

### **Surveillance and Detection**

\*Attack Warning: early warning, detection, or recognition of biological weapons attacks is necessary for a timely response to mitigate potential consequences. Dispersal characterization and recognition methods are under development and revision of existing systems at federal, state, local, and international levels for early warning and protection human and animal populations, food, water, agriculture, and the environment.

Attribution: National Bioforensic Analysis Center, part of the NBA and Countermeasure Center, DHS, serves as lead for technical forensic analysis and interpretation of information.

### **Response and Recovery**

Once an attack is detected, the speed and coordination of government, private and international responses will be critical for mitigating the lethal, medical, psychological, and economic consequences will be dependent upon pre-attack planning and preparedness, capabilities to treat casualties, risk communications, physical control measures, medical countermeasures, and decontamination capabilities.

Response Planning: DHS is drafting an annex for NRP for a biological response which will serve as a catalyst to state and local government planning. Mutual aid and interagency agreements will be in place for plausible threat assessments. Plans are to be

## Homeland Security Presidential Directives (HSPD) Summary

regularly tested

Mass Casualty Care: Prevention through rapid treatments (antibiotics and vaccines) could save lives, protect scarce medical resources, preserve social order, and reduce costs. State and Local public health officials are working with the Administration on a quick distribution, to expand or create new federal, state, local capabilities for all hazards. DHHS, lead for coordinating all federal assets while augmentation of medical and public health while DHS remains overall in command of event with coordination as necessary Veteran's Affairs and Transportation.

Risk Communication: DHS is developing a coordinated, long-term scale communication strategies, plans, products, and channels to reach all societies, including those with physical or language limitations. The efforts will provide quick resources for calming and informing the public on the situation, what can be expected and to stay safe or evacuate.

Medical Countermeasure Development: The National Institutes of Health (NIH) under DHHS, with DHS, DOD, and others are enhancing an aggressive research program for better medical countermeasures to prevent illness, build new labs to ensure assessments stay ahead of threats. DHHS has lead with other agencies to ensure safe medical countermeasures are developed.

Decontamination: Recovery may include decontamination and remediation. State and local governments are to look at existing capabilities to rapidly assess, decontaminate, and return to pre-attack activities. Federal capabilities are being assessed and standards and protocols are under development.

EPA Administrator coordinates with the AG and Secretaries of Defense, Agriculture, Labor, Health and Human Services, and DHS in development of specific standards, protocols, and capabilities for contamination risk and developing strategies, guidelines, and plans for decontamination of persons, equipment, and facilities.

HSPD 11

August 27, 2004

### **Comprehensive Terrorist-Related Screening Procedures**

An enhanced screening strategy plan to be developed through comprehensive, coordinated procedures that detect, identify, track and interdict people, cargo conveyances, and other entities and objects that pose threats while maintaining safeguards for legal rights, freedoms, civil liberties, and information privacy, building upon existing risk assessment capabilities, inspections, credentialing and commerce activities. Implement this screening approach in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure to be effective, maintain existing protective measures that are innovative, flexible, build upon existing systems and best practices; integrate, consolidate, and eliminate duplicative systems; enhance information flow; limits delays; provide protocols and training (refresher and updates) for screening people, cargo, and conveyances; understand the consequences. This builds upon HSPD-6. Identifying skills

## Homeland Security Presidential Directives (HSPD) Summary

and training, frequency and how to incorporate sharing and known traveler screen options. Terrorist Screening Center Database at the Terrorist Threat Integration Center and DHS includes protection.

HS Secretary, along with the AG, Secretaries of State, Defense, Transportation, Energy, Health and Human Services, Commerce, and Agriculture, the Directors of Central Intelligence and OMB and other federal departments submit through the Assistant to the President for HS.

The Strategy Plan is to be an annual or as necessary document to include a prioritized investment and implementation plan for a systematic approach to screening that optimizes detection and interdiction of terrorists with description of the scope, sharing of information, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities to implement this screening policy.

HSPD 12

August 27, 2004

### **Policy for a Common Identification Standard for Federal Employees and Contractors**

Secured facilities require standards to ensure quality, enhance security, increase efficiency, reduce identity theft, and protect personal privacy with a mandatory criteria, for staff and contractors. Secretary of Commerce shall promulgate a federal standard in coordination with Secretary of State, Defense, AG, DHS, OMB and the director of the Office of Science and Technology policy, updating as necessary.

Cards based on sound criteria for individual employee verification; resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; rapid electronic authentication, and issued by reliable providers. The standards to have graduated criteria but will not apply to ID under 44 USC 3542(b)(2). Privacy Act 5 USC. 552a.

HSPD 13/ NSPD-43

December 21, 2004

### **Maritime Security Policy**

Established policy, guidelines and implementation actions to enhance and protect national efforts with federal, state, local, and private sector entities. Establishes a Maritime Security Policy Coordinating Committee to coordinate interagency efforts.

Background: Maritime Domain means all areas in and around water and ports with all federal, state, local and private partners which covers large expanse of potential exploitation yet safeguarding international trade, economic cooperation, and free flow commerce. Maritime policy is to use all US laws, treaties and other international agreements

Protect U.S. population centers, critical infrastructure, borders, harbors, ports and coastal approaches. Expedite response and recovery. Maximize security awareness in support of US forces. Establishes the Maritime Security Policy Coordinating Committee, consistent with NSPD and HSPD-1. MSPCC serves as a regional coordination forum for existing interagency practices, coordination, and execution of US policies and strategies related to

## Homeland Security Presidential Directives (HSPD) Summary

maritime security, as well as new initiatives for consideration by the NSC and HSC. Co-chairs may invite others as they deem appropriate.

MSPCC co-chair by an NSC staff selected by the Assistant to the President for National Security Affairs and a HSC representative selected by the Assistant to the President for HS and include:

The Vice President; Secretary of State; Secretary of the Treasury;  
The Secretary of Defense; Attorney General; Secretary of Interior;  
The Secretary of Commerce; Secretary of Transportation; Secretary of Energy;  
The Secretary of Homeland Security; Director, Office of Management and Budget;  
The United States Trade Representative; Director of Central Intelligence  
Chairman of the Council on Environmental Quality; Chairman of the Joint Chiefs of Staff;  
Director, Federal Bureau of Investigation; Director, National Counterterrorism Center

National Strategy for Maritime Security. Integrated and coordinated strategy led by Secretaries of Defense and Homeland Security to cover domestic, international, public and private components with adjustment for global and other issues or threats; built upon existing policies.

### Maritime Domain Awareness

Co-chairs, Secretaries of Defense and HS, established the Maritime Domain Awareness Senior Steering Group and other federal agencies join in for participation with near and long-term objectives, resources and recommendations for change.

Global Maritime Intelligence Integration. Secretary of Defense and Homeland Security with the Director of Central Intelligence in coordination with the Director of the National Counterterrorism Center, and director of the Federal Bureau of Investigation identify critical data to share.

Domestic Outlook: A successful strategy to implement this directive must include state and local government and consultation with private sectors. HS Secretary, with the AG and Secretaries of Treasury, Interior, Commerce, and Transportation will coordinate and implement this plan.

Coordination of International Efforts and International Outreach. Secretary of State shall lead this global effort for policies, programs, and initiatives for implementation and plan approval. Domestic Outreach: strategy to include coordination with state and local authorities and private Secretary of State with Secretary of Defense, Commerce, Transportation, and Homeland Security and the US Trade Representative with private sectors.

Maritime Threat Response: The Secretaries of Defense and Homeland Security with the AG, Secretaries of State, Treasury, Commerce, and Transportation, shall develop a comprehensive National Maritime Security Response Plan to be approved by the President. (supplements HSPD-5 and complements HSPD-7 as required by HSPD-8) To indicate lead agency roles and responsibilities and changes to PDD-39 and 62 for

## Homeland Security Presidential Directives (HSPD) Summary

maritime security response and counterterrorism operations; maritime interception operations; prevention and detection of and response to the mining of US ports; 4) detection, interdiction, and disposition of targeted cargo, people and vessels; 5 attacks on vessels with US citizens aboard or affect US interests anywhere. Protocols, recommendations are to be included within the plan.

**Maritime Infrastructure Recovery:** Rapid recovery is critical to the economic well being of the US. Having a strong economy serves as a deterrent. HS Secretary with the Secretaries of Defense, State, Treasury, Interior, Commerce, and Transportation along with key industry stakeholders shall develop standards for recover operations and a plan with an exercise program consistent with the National Exercise program, complementary to HSPD-8. Focus shall be on restoration of physical assets and transportation systems and be approved by DHS. Program must be similar and consistent to

**Maritime Transportation System Security:** HS Secretary with Secretaries of Defense, State, Commerce, and Transportation and the US Trade Representative with industry representatives. Recommendations may improve regulation, such as the national and international regulatory licensing, carriage, communications, safety equipment, and other critical systems for private vessels, including commercial vessels with the Assistants to the President for National Security Affairs and Homeland Security.

**Maritime Commerce Security:** Need to promote global supply chain security practices with HS Secretary leading along with Secretaries of Defense, State, the Treasury, Commerce, Transportation, and Energy with US Trade Representative along with appropriate industries. Point-to-point tracking built on existing resources and framework.

HSPD 14/NSPD 43

April 15, 2005

### **Domestic Nuclear Detection**

To avoid unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the US, continue to deploy and enhance detection capabilities for federal, state, local, and tribal governments and the private sector, balancing use and ownership with research and detection. HS Secretary, with the Secretaries of State, Defense, Energy, AG, shall establish a national level Domestic Nuclear Detection Office (DNDO) within DHS. DNDO is to include DHS, DOD, DOE, DOS, Justice (DOJ), and other federal Departments and agencies as appropriate. Under section 102 (a) (2) of HS Act of 2002: Serve as primary entity in US to develop, acquire, and support the deployment of domestic system to detect and report on attempts to import transport or use unauthorized nuclear and improve over time. Federal, state and local and tribal detection. HS Secretary, AG and the Secretaries of Defense and Energy, additional protocols and procedures to ensure appropriate officials know who should respond for law enforcement, military, emergency response, or other authorities.

Develop with HS Secretary in coordination with the Attorney General and Secretaries of State, Defense, Energy an enhanced global nuclear detection architecture and intelligence

## Homeland Security Presidential Directives (HSPD) Summary

analysis, under the DNDO; Secretary of Defense will implement DOD requirements within and outside the US and Secretaries of State, Defense, and Energy will maintain their global architecture outside the US. Research and development efforts to aggressively implement appropriate information flow, including foreign governments. State, Defense, Energy and HS and AG shall provide appropriate nuclear, scientific, and other expertise to the DNDO, participate in joint development and coordination of detection and response guidance, protocols, and training for federal, state, local, and tribal officials; participate in developing and coordinating global nuclear detection

Energy Secretary shall lead development of nonproliferation research and development look at dual-use research for domestic nuclear and radiological diction and shall include test and evaluation, deployment equipment procedures, maintaining awareness of foreign sensitivities and sharing with other agencies.

DOD Secretary shall consult with HS Secretary on all DNDO's issues to ensure efficiencies, interoperability, and sharing of innovative concepts and operational procedures.

The AG shall coordinate with HS Secretary on DNDO's global nuclear detection architecture in relation to development of protocols, training and sharing information. This complements the AG's role in HSPD-5.

Secretary of State shall coordinate with the HS Secretary on DNDO's global nuclear detection architecture, especially for overseas detection and reporting.

Director of National Intelligence (DNI) shall coordinate with HS Secretary on DNDO's architecture and ensure timely dissemination to DNDO of all radiological, nuclear, and related threats. CI Director works until DNI is appointed.

Atomic Energy Act of 1954; Homeland Security Act of 2002; National Security Act of 1947 (all as amended); Presidential Guidance; Subject to appropriations

HSPD 15/ NSPD 46      classified

March 2006

### ***[on the war on terrorism]***

Defense Secretary Donald Rumsfeld, in a foreword to the document, wrote that the plan provides guidance "for cooperation with other U.S. government departments and agencies and with collation partners for planning and conducting military operations."

Penned under the direction of Army Brig. Gen. Robert Caslen, deputy director for the war on terrorism on the Joint Staff, the strategy sets forth six objectives in the push to "defeat terrorist extremism as a threat to our way of life and create a global environment inhospitable to terrorist extremists."

Those objectives are: deny terrorists the resources they need to operate and survive;

## Homeland Security Presidential Directives (HSPD) Summary

enable partner nations to counter terrorism; deny proliferation of weapons of mass destruction, recover and eliminate uncontrolled materials, and maintain a capacity for consequence management; defeat terrorists and their organizations; counter state and non-state support for terrorism in coordination with other U.S. government agencies and partner nations; and contribute to the establishment of conditions that counter ideological support for terrorism.

**“President Issues ‘War on Terror’ Directive to Improve Government Coordination. *March 8, 2006.* The INSIDER. InsideDefense.com.**

The agreement states, “‘Maritime warning’ consists of processing, assessing, and disseminating intelligence and information related to the respective maritime areas and internal waterways of, and the maritime approaches to, Canada and the United States, and warning of maritime threats to, or attacks against North America utilizing mutual support arrangements with other commands and agencies, to enable identification, validation, and response by national commands and agencies responsible for maritime defense and security. Through these tasks NORAD shall develop a comprehensive shared understanding of maritime activities to better identify potential maritime threats to North American security. Maritime surveillance and control shall continue to be exercised by national commands and, as appropriate, coordinated bilaterally.”

The agreement also emphasizes intelligence and information sharing and includes “confirmation of NORAD’s ability to conduct information operations,” according to the Canadian government’s explanatory memorandum included with the agreement. Information operations are not defined in the updated agreement and the Canadian statement. NORAD updated in May 2006.”

HSPD 16/ NSPD 47 [on aviation security and threats to commercial aircraft] June 22, 2006

HSPD 18 Medical Countermeasures Against Weapons of Mass Destruction January 31, 2007

The National Strategy to Combat Weapons of Mass Destruction (December 2002) and Biodefense for the 21<sup>st</sup> Century (April 2004) identify response and recovery for a WMD attack. Medical countermeasures are guided by anticipation, intervention, and logistical acquisition that is supportable at the federal, state, and local asset level (4). Biological threats are the greatest opportunity for medical mitigation. Creating defenses to mitigate each of the catastrophic CBRN threats will need to remain flexible to address future challenges.

Risk assessment from the life science, consequence management, public health, law enforcement, and intelligence communities should be integrated for identification and determination of countermeasures (11a) with primary focus on high-risk (11b) with assistance from homeland security, intelligence, first responder, and the private sector for the product development life cycle (14). The DHHS has the lead for setting the medical countermeasure requirements and to coordinate the research, development and procurement activities and committee. A strategic plan for the risks and life-cycle will be developed by Spring 2007. Academia, private sector and nongovernmental entities are to

## Homeland Security Presidential Directives (HSPD) Summary

be included within the entire process.

HSPD 19 Combating Terrorist Use of Explosives in the United States February 12, 2007

Creates a national policy to develop a national strategy and implementation plan regarding terrorist's use of explosives in the United States. Implementation will result in an explosive attack detection, prevention, prevention, protection, or response activities directive and recommendations for all partners to identify capabilities.  
FBI's National Threat Warning System (NTWS)

\*Numbers in parentheses (or other indices) relate to the specific number in the HSPD.

## Homeland Security Presidential Directives (HSPD) Summary

### National Preparedness System

Strategy	Presidential Directives	National Guiding Documents	Results
<p>The National Strategy for Homeland Security</p> <p>7 National Priorities:</p> <ul style="list-style-type: none"> <li>• Implement the National Incident Management System and National Response Plan</li> <li>• Expand Regional Collaboration</li> <li>• Implement the National Infrastructure Protection Plan</li> <li>• Strengthen Information Sharing and Collaboration Capability</li> <li>• Strengthen Interoperable Communications Capabilities</li> <li>• Strengthen CBRNE Detection, Response, and Decon Capabilities</li> <li>• Strengthen Medical Surge and Mass Prophylaxis Capabilities</li> </ul>	<p>HSPD-5 {</p> <p>HSPD-7 {</p> <p>HSPD-8 {</p>	<ul style="list-style-type: none"> <li>• National Response Plan (NRP)</li> <li>• National Incident Management System (NIMS)</li> <li>• National Infrastructure Protection Plan</li> <li>• <b>National Preparedness Goal</b></li> <li>• National Planning Scenarios</li> <li>• Universal Task List (UTL)</li> <li>• Target Capabilities List (TCL) + Levels</li> <li>• Homeland Security Grant Program Guidance</li> <li>• National Preparedness Guidance</li> </ul>	<p>Common Approach to National Incident Management</p> <p>Common National Approach:</p> <p>Prevention Protection Response Recovery Preparedness</p>

### DRAFT DRAFT DRAFT WASHINGTON STATE PREPAREDNESS

		<ul style="list-style-type: none"> <li>• Comprehensive Emergency Management Plan</li> </ul>
		<ul style="list-style-type: none"> <li>•</li> </ul>
All disasters are local.		

Need to add information on PD 47 and PD 16 (12/06). Need to adjust with the FEMA changes to occur.

2006: Military Department State Strategy  
 Federal base plan: National Response plan  
 State base plan = CEMP