

CHAPTER I

INTRODUCTION

September 11, 2001 will remain a tragic day for the United States of America and the rest of the civilized world. In response to terrorist attempts to demoralize and frighten the American public, the United States Government responded with immediacy and resolve. Among the many necessary and appropriate responses was the October 8, 2001 issuance of Executive Order 13228¹ by United States President George W. Bush. Through Executive Order 13228, President Bush firmly established the Office of Homeland Security (OHS) with a clear and critical mission “to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.”

To assure the success of the OHS mission, President Bush signed Homeland Security Presidential Directive-3 (HSPD-3)² on March 12, 2002, calling for the creation of the Homeland Security Advisory System (HSAS).

The purpose of this report is to provide guidance for the development of the HSAS and is a reflection of the combined views of government officials at all levels, public interest groups and the private sector as required by HSPD-3. This report addresses: considerations for the assessment and assignment of Threat Conditions; issues regarding the development of Protective Measures which correspond to individual Threat Conditions; information delivery systems for the dissemination of Terrorism Threat Warnings; and findings related to the 45-Day Comment and Review Period.

Until final legislative decisions are made regarding the proposed Department of Homeland Security, or until new Presidential Directives are issued which substantively change HSPD-3 requirements, **it is recommended that this report serve as the complete recommendations by the Attorney General of the United States to the President for proposed refinements to the Homeland Security Advisory System as directed in HSPD-3.**

The HSAS is the first national terrorist threat level warning system in the United States and will "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." This system provides warnings in the form of graduated "Threat Conditions" that elevate along a five-tier structure as the risk the threat increases. Furthermore, all executive branch departments, agencies and offices are required to implement a corresponding set of predetermined "Protective Measures" for each Threat Condition, to further reduce vulnerability and increase response capability during a period of heightened alert.

¹See Appendix A for Executive Order 13228.

²See Appendix B for Homeland Security Presidential Directive-3.

Cornerstones for Success

In establishing the OHS, President Bush identified several cornerstones upon which the structure and success of the organization will be supported:

1. ***Prevention.*** OHS is tasked with coordinating national efforts to prevent terrorist acts within the United States. This will require OHS to form strong bonds with the appropriate Federal, State, local agencies, and private concerns to facilitate the exchange of information relating to immigration and visa matters, shipments of cargo, and preventing the entry of terrorist materials and supplies into the United States. In addition to preventing the entry of terrorists and their supplies into the United States, the OHS is charged with coordinating efforts to remove such terrorists from the United States when they are found.

2. ***Preparedness.*** OHS is tasked with coordinating national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States. In order to accomplish this task, OHS will interact with appropriate Federal, State, local agencies, and private industry and organizations who have similar missions, thereby ensuring the best possible plans are brought forth for the American public.

3. ***Protection.*** Perhaps the most critical challenge in the wake of September 11th is to ensure the American public that all is being done to prevent further terrorist events. In that regard, OHS is tasked with coordinating all efforts to protect the United States and its critical infrastructure from the consequence of terrorist attacks. Success is incumbent upon the continued cooperation between all appropriate Federal, State, local agencies, and private concerns.

4. ***Detection.*** OHS has been tasked to identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. Under the coordination of the Assistant to the President for National Security Affairs, OHS is further tasked to identify priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States.

5. ***Response and Recovery.*** There is to be a coordination of all efforts to respond to and promote recovery from terrorist threats or attacks within the United States. As with the other cornerstones, this will require the continued cooperation between all appropriate Federal, State, local agencies, and private concerns. All efforts will be made to ensure the rapid restoration of such critical infrastructures as transportation, energy, telecommunications, financial markets, and medical infrastructures, to name a few, following a terrorist attack. Also, all efforts will be made to coordinate the critical response by appropriate agencies to contain and remove biological, chemical, radiological, explosive, or other hazardous materials in the event of a terrorist threat. In the event of a terrorist attack involving such hazardous materials, all effort to mitigate the effects of such an attack will be coordinated by the OHS.

6. ***Incident Management.*** The Assistant to the President for Homeland Security has been designated as the individual primarily responsible for coordinating the domestic response efforts for all departments and agencies in the event of an imminent terrorist threat and during the immediate aftermath of a terrorist attack within the United States.

It should be noted that all efforts expended by the various government agencies tasked with the most important duties of preventing, preparing, protecting, detecting against, as well as responding to and recovering from terrorist threats will be in vain unless there is timely, accurate and clear communication to the widest appropriate audience possible.

Never before has such an effort been undertaken to bring together all executive departments and agencies, State and local governments, along with private entities, to ensure this national strategy succeeds. The recommendations provided in this document, if adopted, will constitute the Homeland Security Advisory System. The importance of the continual need for review and revision of this system cannot be overemphasized. The success of the HSAS will ultimately depend upon a continuously constructive dialog between all contributing members of the OHS, to include the citizens of the United States of America.

CHAPTER II

THREAT CONDITIONS AND PROTECTIVE MEASURES

Executive Branch Requirements

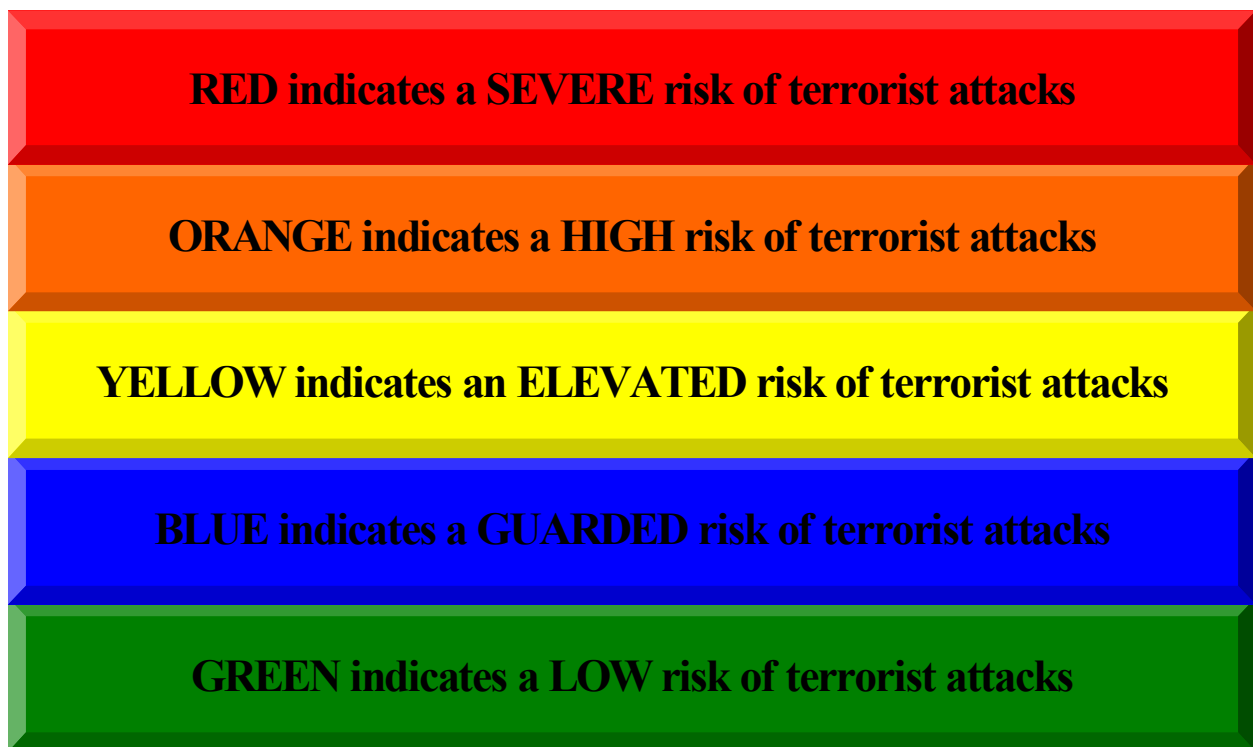
The HSAS's intended purpose is to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State and local authorities and to the American people. The HSAS is intended to create a common vocabulary, context, and structure for an ongoing national 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. According to HSPD-3, the HSAS is binding on executive branch agencies and departments. Specifically, HSPD-3 states that “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.” HSPD-3 states that HSAS Threat Conditions shall be assigned by the U.S. Attorney General in consultation with the Assistant to the President for Homeland Security. HSPD-3 also directs the Attorney General to seek the views of the appropriate Homeland Security Principals, or their subordinates and other parties as appropriate, regarding Threat Condition designation unless exigent circumstances dictate otherwise. The President’s initiative to establish the Department of Homeland Security proposes a shift in the responsibility for assignment of Threat Conditions and management of the HSAS to the Secretary of Homeland Security. Therefore, **it is recommended that legislation establishing the Department of Homeland Security include language that requires the Attorney General of the United States be consulted in the assignment of future Threat Conditions.**

The HSAS utilizes a set of graduated Threat Conditions that would increase as the risk of the threat increases. HSPD-3 requires that with each Threat Condition, executive branch departments and agencies implement a corresponding set of Protective Measures to further reduce vulnerability or increase response capability during a period of heightened alert. HSPD-3 also states that executive branch department and agency heads are responsible for developing and implementing their own Protective Measures and other antiterrorism or self-protection and continuity plans. These agencies and departments are also responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack, to include resourcing, rehearsing, documenting, and maintaining their anti-terrorism or self-protection and continuity plans. **It is recommended that the HSAS serve as the national framework for State and local government agencies and private industry, and that the OHS encourage these organizations to emulate the HSAS, making further enhancements as needed to meet specific community and business requirements.**

Threat Conditions

Threat Conditions characterize the risk of terrorist attack. The HSAS establishes five Threat Conditions each identified by a description and corresponding color. The colors and associated risk levels, from highest to lowest, are as follows:

HSAS Threat Conditions



Threat Conditions may be assigned for the entire nation, or they may be set for a particular geographic area or industrial sector. HSPD-3 requires regular periodic reviews of the

designated Threat Condition to determine if adjustments are warranted. HSPD-3 further stipulates that "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." HSPD-3 also clarifies that "every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation."

A large percentage of the reviewed public comments indicate a degree of confusion when distinguishing or interpreting colors and corresponding risk descriptions. Therefore, **it is recommended that whenever Threat Conditions are posted, the condition be clearly indicated with both the color-coding and risk description.**³

Protective Measures

HSPD-3 states, "the assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures." Protective Measures are described in HSPD-3 as "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 are delegated by HSPD-3 to individual Federal department and agency heads. Furthermore, HSPD-3 requires that Federal department and agency heads submit an annual written report to the President of the United States, through the Assistant to the President of Homeland Security, describing the steps their departments or agencies have taken to develop and implement appropriate Protective Measures for each Threat Condition.

Although ultimate responsibility is delegated to department and agency heads to develop department and agency-specific Protective Measures, the OHS suggests incorporating the following general measures into their plans as they correspond to their respective Threat Conditions:

RED - SEVERE THREAT CONDITION

- ▶ In addition to all Protective Measures of Orange (High Risk), Yellow (Elevated Risk), Blue (Guarded Risk) and Green (Low Risk)
- ▶ Assign emergency response personnel and pre-position specially trained teams;
- ▶ Monitor, redirect or constrain transportation systems;
- ▶ Close public and government facilities; and
- ▶ Increase or redirect personnel to address critical emergency needs.

ORANGE - HIGH THREAT CONDITION

- ▶ In addition to all Protective Measures of Yellow (Elevated Risk), Blue (Guarded Risk) and Green (Low Risk)
- ▶ Coordinate necessary security efforts with armed forces or law enforcement agencies;

³See Appendix C for FBI Field Office Survey graphs.

- ▶ Take additional precautions at public events;
- ▶ Prepare to work at an alternate site or with a dispersed workforce; and
- ▶ Restrict access to essential personnel only.

YELLOW - ELEVATED THREAT CONDITION

- ▶ In addition to all Protective Measures of Blue (Guarded Risk) and Green (Low Risk)
- ▶ Increase surveillance of critical locations;
- ▶ Coordinate emergency plans with nearby jurisdictions;
- ▶ Assess further refinement of protective measures within the context of the current threat information; and
- ▶ Implement, as appropriate, contingency and emergency response plans.

BLUE - GUARDED THREAT CONDITION

- ▶ In addition to all Protective Measures of Green (Low Risk)
- ▶ Check communications with designated emergency response or command locations;
- ▶ Review and update emergency response procedures; and
- ▶ Provide public with necessary information.

GREEN - LOW THREAT CONDITION

- ▶ Refine and exercise preplanned Protective Measures;
- ▶ Ensure personnel receive training on HSAS, departmental, or agency-specific Protective Measures; and
- ▶ Regularly assess facilities for vulnerabilities and take measures to reduce them.

Private Industry and American Public Considerations

HSPD-3 makes clear that executive branch department and agencies "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." However, HSPD-3 states specifically that the HSAS is only binding on the executive branch and *suggested*, although voluntary, to other levels of government and the private sector. To this end, the American Red Cross continues to prepare and distribute numerous documents which provide beneficial recommendations to the American public and private industry regarding disaster preparedness and response plans.⁴ These recommended actions were developed specifically for various audiences to include individuals, families, neighborhoods, schools, and businesses. Furthermore, the recommended actions provided by the American Red Cross correspond to the HSAS⁵ and

⁴See Appendix D for list of American Red Cross Materials for Use with Homeland Security Advisory System.

⁵See Appendix E for American Red Cross Homeland Security Advisory System Recommendations.

appropriately guide its users to published resources such as the American Red Cross brochure titled *Terrorism: Preparing for the Unexpected*.⁶ **It is recommended that the American public and private industry be encouraged to utilize the HSAS, and American Red Cross publications, to facilitate the development of Protective Measures for their own specific requirements.**

⁶ See Appendix F for a copy of American Red Cross brochure titled “Terrorism: Preparing for the Unexpected.”

CHAPTER III

ASSIGNMENT OF THREAT CONDITIONS

Threat Condition Considerations

HSPD-3 and the FBI's National Threat Warning System (NTWS)⁷ provide appropriate factors for the assignment of threat conditions. The NTWS incorporated and expanded the earlier Terrorist Threat Warning System (TTWS), which was established by the Attorney General on October 13, 1989. The NTWS ensures that vital information regarding terrorism reaches the U.S. counterterrorism and law enforcement communities. The guidelines governing the NTWS also provide specific policy regarding public notification procedures. Currently, the NTWS includes language that categorizes disseminated messages into three types: alerts, advisories and assessments. The HSAS does not make these distinctions and, therefore, the NTWS language is being revisited to ensure consistency with the HSAS so as not to cause confusion to the receiving audiences.

HSPD-3 and NTWS guidelines both agree to certain criteria which should be considered when assessing threat risks. A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, more than quantitative calculation. Higher Threat Conditions indicate greater risk of terrorist act, with risk including both probability and gravity. One important factor in determining a threat risk is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

- The credibility of the threat.
- The level of corroboration regarding the threat.
- The degree to which the threat is imminent.
- Threat specificity, to include a specific target.
- The gravity of the consequences if threat is delivered.
- The assessed vulnerability of the target.

Assessing Threat Credibility and Imminency

Factors that determine the credibility of a threat include, but are not limited to, the following considerations:

- The source of the threat.
- Source dependability, to include source's historical record.
- Source reliability.
- Credibility of the source's access to certain information.
- Purpose and objective of the terrorist group in question.

⁷See Appendix G for National Threat Warning System document.

- Capability and resources of the terrorist group in question.
- Specificity of source's information.

Corroboration of Threat

To corroborate a threat, the following questions should be determined through existing intelligence resources:

- Does the threat serve the stated or philosophical purpose of the group?
- Does intelligence reporting indicate movement or activity in a threat area?
- Do other information resources point to the same preliminary threat conclusions?

Target Vulnerabilities and Consequences

Terrorist threats range from disruptive vandalism, to catastrophic attacks effecting large centers of population and vital infrastructure. With a specific threat of a terrorist attack it is necessary to determine what consequences would be realized if an attack were to occur. Some of the questions to be considered are as follows:

- Is the target strategically significant as to pose a major disruption to vital services and/or a loss of life?
- How would Federal, State and local governments, along with private industry and the American public, react to the loss and/or disruption of a particular target?
- If the threat is imminent, how much time exists for countermeasures to be implemented?
- Can a target be made less attractive through enhanced security measures?
- Can the threat be intercepted and neutralized by law enforcement or other U.S. Government resources?
- Can the affected parties be warned and counter-measures implemented prior to the attack, thus averting a loss of life?

At every Threat Condition level, the same assiduous attention to threat assessment methodology will be applied. **It is recommended that all HSAS education and awareness programs emphasize that despite the best decision to assign an appropriate Threat Condition, there can be no guarantee that a terrorist attack will be prevented.**

CHAPTER IV

INFORMATION DELIVERY SYSTEMS

Homeland Security Presidential Directive-3 (HSPD-3) calls for the identification of those systems that will be utilized by the Federal, State and local government officials, to communicate threat information. The nation requires a Homeland Security Advisory System (HSAS) 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. The system set forth will provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases.

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.

A threat is defined by PDD-39, and the Attorney General Guidelines, as any indication of planned violence against U.S. persons or facilities, including any persons or facilities located in the United States or damage to the U.S. national security or infrastructure, including computer networks. A threat can originate from individuals, terrorist groups, or other criminal elements.

FEMA has been tasked by OMB, via the Office of Homeland Security, to develop and implement a system within the next 18 to 24 months, which will become the Homeland Security Advisory System's primary means of information delivery. The Disaster Management e-Government initiative will result in the development of a web-based application which will be capable of issuing national alert notifications for all hazards via multiple communication channels and devices. It will become part of the suite of applications enabled by FEMA's disaster management portal, entitled "DisasterHelp.gov", which will be available to private citizens, businesses, non-government organizations, all local, State, and Tribal government entities, as well as the Federal government. It will be a "one-stop" full service gateway providing an open technology forum with wide access to relevant information, including Sensitive but Unclassified (SBU) material.

Until the development and implementation of this new system occurs, certain information delivery systems, currently in place, have been identified as the most effective and efficient means with which to ensure the most timely and thorough information dissemination coverage as possible. While it may appear that some of the systems are redundant, it is far more important to ensure that the widest possible audience is reached when disseminating threat information. **It is recommended that all current information dissemination systems identified in this report be adopted as those that will be utilized to disseminate threat information as called for under HSPD-3. These systems will be utilized until such time that a more permanent and all-inclusive system is perfected by which threat information will be disseminated community and nationwide.**

The following intentionally redundant information dissemination systems described below, can be utilized to reach an increasing audience size depending upon the information to be disseminated. If the determination is made to disseminate threat information and/or to adjust the threat level, the initial target audience will most likely be key federal agencies whose mission includes national defense, disaster response/recovery, and intelligence related functions. The Automated Digital Network (AUTODIN) and Defense Messaging System (DMS) are the systems which will be utilized to accomplish this initial dissemination. These systems are in compliance with Executive Order 12656, which requires that all federal government agencies be able to communicate and interoperate with each other in times of national crisis. AUTODIN software is utilized by each federal agency to send messages via teletype. Each teletype is addressed to the appropriate receiver by consulting the Allied Routing Indicator Book, which contains the addresses for all federal agencies and their components. AUTODIN is capable of sending messages up to Top Secret/SCI.

AUTODIN is scheduled for full replacement by DMS in all federal agencies by the end of 2003. DMS will also be able to handle messages up to Top Secret/SCI, but will allow individual users to send e-mails to other desktop computers of any other user within the federal government. Essentially, messages could feasibly reach up to 5 million users utilizing the DMS software worldwide.

Should the decision be made to increase the size of the audience to include all state and local law enforcement, or a selected portion thereof, then the National Law Enforcement Telecommunications System (NLETS) would be the vehicle utilized to deliver the message. An NLETS terminal is required to accomplish this. The dissemination is prepared by the Federal Bureau of Investigation (FBI) and is sent out via the NLETS terminal located at FBI headquarters.

There are two systems which can serve to reproduce and further disseminate the NLETS message, thus ensuring saturation. The Regional Information Sharing Systems Program (RISS) and the Law Enforcement On-Line (LEO) systems will allow the user to retransmit the NLETS message via e-mail and facsimile to a set of predetermined recipients.

If the decision is made to also include all state and local emergency services, or any portion thereof, then FEMA has the systems in place to make the appropriate contact and dissemination. The appropriate threat-warning message with instructions will be furnished directly to FEMA's Operations Center at Mt. Weather. FEMA can disseminate the message to many different audiences utilizing several different systems, as appropriate. These systems are further identified and defined herein.

Should the decision be made to disseminate the information to various private industries, including but not limited to critical infrastructure industries, then the systems in place at the National Infrastructure Protection Center (NIPC) would be utilized. The message would be sent to NIPC for transmittal preparation in the proper format, and the appropriate system would be

used to transmit the message. For example, a critical infrastructure industry would be reached via the Information Sharing and Analysis Center (ISAC). The NIPC systems are further identified and defined herein.

If it is determined that the information is going to be made available to the general public, then the best method for dissemination would be via appropriate news conference utilizing all available public media outlets. An appropriate message should be delivered, via the Office of Homeland Security (OHS) website, to the public at large as well as all other federal, state and local agencies. All federal, state and local agencies should be strongly encouraged to reproduce this message for posting on their own public websites. Precise instructions should be disseminated requiring all agency public websites to reproduce the message with the exact same wording as the OHS message to ensure that conflicting information/instructions are not given. Failure to do so could potentially result in unnecessary and counterproductive public confusion.

The identified information dissemination systems include:

FEDERAL GOVERNMENT

Delivery Systems: AUTODIN/ DMS, COMMUNICATOR!, WAWAS, “BLAST” Conference

AUTODIN: Department of Defense's Automated Digital Network⁸

DMS: Defense Messaging System

Coverage: All federal government agencies, Department of Defense entities, and U.S. embassies worldwide.

Information capability: Unclassified up through TS/SCI.

System administrator: DOD and FBI

AUTODIN Miscellaneous information: The Automated Digital Network (AUTODIN) uses the FBI's Secure Automated Message Network (SAMNET) to connect to AUTODIN users. In keeping with its responsibilities under the NTWS, the FBI's Counterterrorism Division (CTD) currently communicates threat warnings to the rest of the Federal government through AUTODIN. Most U.S. government agencies are a part of the AUTODIN, and communications are sent out with appropriate addresses unique to each receiving agency. Once the original message has been sent out to the appropriate federal agencies, it is incumbent upon those agencies to disseminate the message throughout their own organization utilizing the information dissemination system(s) already in place within the agency.

DMS Miscellaneous information: AUTODIN is scheduled for replacement by the Defense Messaging System (DMS), which brings with it new message and communication protocols, new addressing, new security, and new procedures. These changes will dramatically impact the

⁸ See Appendix H for AUTODIN and DMS document.

exchange of classified messages with external agencies, both inbound and outbound. All government agencies are required to utilize the DMS by the end of 2003. There will be two types of DMS users, individual and organizational. Individual users are those who send and/or receive routine administrative messages on their own behalf. Organizational users are those who are authorized to send and/or receive official Command and Control message traffic on behalf of their organization. This different messaging capability is one of the great benefits of DMS and a distinct advantage over AUTODIN. As an Individual user, one can send a message to an individual or to several individuals at one time, called a vertical message. An Organizational user can send a message across multiple organizations at one time, called a horizontal message. This will be the type utilized for the NTWS.

COMMUNICATOR!: Automated Voice Notification System.

Coverage: All Federal Agencies.

Information capability: Unclassified.

System Administrator: FEMA

Miscellaneous information: The COMMUNICATOR! is an automated voice notification system which utilizes pagers, cellular phones, work and home telephones to disseminate messages to a pre-determined group of users. These users, when contacted, are directed to call an established toll-free number to receive recorded messages, which are tailored to a given situation. The FEMA Operations Center (FOC) is FEMA's primary, 24-hour Operations Center and as such, directs alert and notification actions through FEMA's network of operations centers. The FOC will use the COMMUNICATOR! system to notify all Federal Departments and Agencies. The FOC will notify the Director, FEMA, the Deputy Director, and the Chief of Staff telephonically, and utilize the COMMUNICATOR! to notify FEMA Assistant and Office Directors, the other Federal Departments and Agencies key staff and national level emergency teams. The FOC will also notify the five Mobile Emergency Response System (MERS) Operations Centers (MOCs) telephonically, who will in turn, use the COMMUNICATOR! to notify Regional Directors and other key regional staff and facilities. Regional Directors will determine activation of Regional Operations Centers (ROCs).

WAWAS: Washington Area Warning and Alerting System.

Coverage: The National Capital region.⁹

Information capability: Unclassified.

System Administrator: FEMA

⁹ See Appendix I for list of WAWAS Members.

Miscellaneous information: The WAWAS is a non-secure, dedicated telephone system for the Washington DC metropolitan area, also called the Emergency Management System. The FOC will relay threat notifications to subscribers over the WAWAS. Subscribers are Federal, State, Local agencies including law enforcement, fire/HAZMAT response and the National Weather Service. Numerous, but not all, Federal agencies currently subscribe to WAWAS. The WAWAS is not tied directly to the National Warning System (NAWAS), however it can be “bridged” at the FEMA Operations Center, in the event an Attack Warning scenario develops. WAWAS has approximately 91 subscribers.

“BLAST” CONFERENCE SYSTEM: Teleconferencing System

Coverage: Federal Departments/Agencies

Information capability: Unclassified.

System Administrator: FEMA

Miscellaneous information: The FEMA Operations Center has a robust “blast” conferencing system. The Conference Arranger allows for pre-loading telephone numbers for grouping and “Blast” conferencing selected parties or groups of individuals. Pre-loaded groups in the system can be activated for a conference within minutes after notification to the FOC. The FOC will relay threat notifications via the “Blast” conferencing system to all Federal Departments and Agencies.

STATE AND LOCAL LAW ENFORCEMENT

Delivery Systems: NLETS, RISS, LEO

NLETS: National Law Enforcement Telecommunications System¹⁰

Coverage: All State and Local law enforcement agencies throughout the United States, and most Federal law enforcement agencies. Approximately 18,000 agencies and 330,000 terminals.¹¹

Information capability: Unclassified up through Law Enforcement Sensitive.

System Administrator: NLETS

Miscellaneous information: NLETS has established a unique message key for the exclusive use of the Homeland Security Awareness System. This unique message key, designated "HS", allows receiving Control Terminal Agencies (CTAs) to distinguish it from a normal

¹⁰ See Appendix J for NLETS document.

¹¹ See Appendix K for list of NLETS Regional Members.

Administrative message, designated "AM". The "HS" message can only be sent by agencies so designated and is delivered with the highest priority allowed by NLETS. Presently, Homeland Security messages are distributed as "AMs", which means that once the message is sent to the State level, a person must read it and decide if further dissemination is warranted to the various users in that State. The "HS" key will bypass this person, and the message will automatically be disseminated throughout the State, or to any group designated by the system. NLETS is a guaranteed message delivery system, and it is estimated that a message with the designation "HS" will take approximately 5 to 10 seconds for nationwide dissemination.

RISS: Regional Information Sharing System¹²

Coverage: Federal, State and Local law enforcement member agencies.

Information capability: Unclassified, with secure e-mail capability.

System Administrator: Any of six multistate regional centers.

Miscellaneous information: Once an NLETS message has been disseminated, it should be reproduced and disseminated to member users via RISS. RISS is designed to enhance the ability of local, state, and federal law enforcement member agencies to identify, target, arrest, and prosecute criminal conspirators. The RISS Program is funded by the Department of Justice's Bureau of Justice Assistance, and consists of six multistate regional centers: Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLLEN), located in Newtown, Pennsylvania; Mid-States Organized Crime Information Center (MOCIC), located in Springfield, Missouri; New England State Police Information Network (NESPIN), located in Franklin, Massachusetts; Rocky Mountain Information Network (RMIN), located in Phoenix, Arizona; Regional Organized Crime Information Center (ROCIC), located in Nashville, Tennessee; and the Western States Information Network (WSIN), located in Sacramento, California. These centers operate in mutually exclusive geographic regions that include all 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. The six centers combined serve over 5,600 local, state, and federal law enforcement member agencies by facilitating and encouraging information sharing and communications to support their investigative and prosecution efforts.

LEO: Law Enforcement On-line¹³

Coverage: Federal, State, and Local law enforcement, criminal justice, and public safety member agencies.

Information capability: Unclassified, with secure e-mail capability.

¹² See Appendix L for RISS document.

¹³ See Appendix M for LEO document.

System Administrator: LEO Network Operations Center.

Miscellaneous information: Once an NLETS message has been disseminated, it should be reproduced and disseminated to member users via LEO. The mission of LEO is to provide electronic communications capabilities that offer a user-friendly format to securely transmit sensitive but unclassified information, throughout the world, to the local, state, and federal law enforcement, criminal justice, and public safety communities. The LEO system provides a vehicle for these communities to exchange information, conduct on-line education programs, and participate in professional special interest and topically focused dialog. As of October 31, 2001, LEO supports a user base of 32,347.

STATE AND LOCAL EMERGENCY SERVICES

Delivery System: NAWAS

NAWAS: National Warning System.

Coverage: All 50 states via state and local warning points.¹⁴

Information capability: Unclassified.

System Administrator: FEMA

Miscellaneous information: NAWAS is a dedicated, two-way nationwide special purpose party line telephone system, which connects to all 50 states to include local warning points. The FOC will broadcast threat notifications via NAWAS and conduct a roll call after the broadcast to ensure receipt by each State. Each state will verify receipt by their local warning points. The U.S. is divided into 10 regions, and each state within the 10 regions has a State Warning Point (SWP). Within each Region, a Regional circuit links the FEMA Regional Office with terminals at all State government warning points. Within each State, an intra-State circuit links State primary and alternate Emergency Operations Centers (EOCs) with each other, the Governors office, and with terminals and extensions at local jurisdictions. State Warning Points are staffed by law enforcement officials and have direct communications to each states governor. The National Weather Service (NWS) is a primary subscriber and has links to their own warning systems for re-broadcast. Currently, there are approximately 1,850 subscribers on the NAWAS system to include U.S. Coast Guard, County, fire and police officials, as well as other emergency response agencies.

PRIVATE INDUSTRY

Delivery Systems: INFRAGARD, ISAC, CERT/CC, and ANSIR

¹⁴ See Appendix N for list of NAWAS Regional Members.

INFRAGARD: Infrastructure Guard¹⁵

Coverage: Federal agencies, business leaders, academic institutions, state and local law enforcement agency members.

Information capability: Unclassified, via secure and public websites.

System Administrator: NIPC (National Infrastructure Protection Center)

Miscellaneous information: The InfraGard program is a nationwide initiative in which all 56 FBI field offices participate by administering to their local InfraGard chapters. Nationally, InfraGard has over 4000 members. It is the most extensive government-private sector partnership for infrastructure protection in the world. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of U.S. critical infrastructures. InfraGard provides a mechanism for the public and private sectors to exchange information pertaining to cyber-intrusion matters, computer network vulnerabilities and physical threats on infrastructures. The FBI provides a secure electronic communications capability to all InfraGard members so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents.

ISAC: Information Sharing and Analysis Center¹⁶

Coverage: Critical infrastructure industries in the sectors of Financial Services, Electric Power, Oil and Gas, Emergency Law Enforcement, Emergency Fire Services, Water, Telecommunications, Information Technology, and representatives covering railroad, aviation, and trucking industries, the computer software anti-virus industry, the chemical industry, and the food industry.

Information capability: Unclassified up through Secret, to cleared members.

System Administrator: NIPC

Miscellaneous information: The NIPC disseminates threat information to the ISACs in three ways. There are daily and weekly teleconferences with the ISACs which constitute the critical infrastructures, i.e. water, oil and gas, and electric power. All pertinent threat information is shared with all sectors during these daily and weekly teleconferences. Information is also disseminated throughout the ISACs via the NIPC Information Bulletin (IB). The IB is issued when there is general threat information, not of an urgent nature but with potential high impact if realized, concerning the private sector. The IBs contain unclassified information and are

¹⁵ See Appendix O for InfraGard document.

¹⁶ See Appendix P for ISAC document in.

disseminated either by NLETS, the NIPC website, and/or e-mail (encrypted or clear). If the IB is sent by e-mail, the recipient is notified by beeper through a preprogrammed, automatic system that an e-mail has been sent. The third manner in which this information is disseminated is called a Sector Notification (SN). An SN is for threat information of a higher significance than an IB. An SN could possibly contain classified information, which is sent via STU III secure facsimile to those ISAC representatives that have received the proper clearances. Again, SNs are delivered via e-mail with the same beeper notification. All ISACs maintain 24-hour coverage seven days a week. Two of the newest ISACs to be formed include the Emergency Fire Services ISAC, which will give NIPC the capability to communicate threat information to the national fire associations, all 50 State Fire Marshals, and over 32,000 local fire and emergency medical departments throughout the nation, and the Food Sector ISAC.

CERT/CC: Computer Emergency Response Team/Coordination Center.¹⁷

Coverage: Computer industry security professionals.

Information capability: Unclassified.

System Administrator: NIPC.

Miscellaneous information: The NIPC and the CERT/CC at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from CERT/CC, including advance Special Communications about impending CERT/CC advisories, upon which CERT/CC seeks NIPC input, as well as weekly intrusion activity information, that it incorporates into strategic and tactical analyses and utilizes as part of its warning function. The NIPC's Watch and Analysis units are routinely in telephonic contact with CERT/CC and the anti-virus community for purposes of sharing vulnerability and threat information on a real-time basis. CERT/CC input is often sought when an NIPC warning is in production. The NIPC also provides information to the CERT/CC, obtained through investigations and other sources, to security professionals in industry and to the public by way of the NIPC Daily Report.

ANSIR: Awareness of National Security Issues and Response program¹⁸

Coverage: Over 30,000 companies in the private sector.

Information capability: Unclassified

System administrator: FBI

Miscellaneous information: ANSIR reaches over 30,000 companies in the private sector, as well as defense contractors, via an ANSIR E-mail system that is supported by LEO. The

¹⁷ See Appendix Q for CERT/CC document.

¹⁸ See Appendix R for ANSIR document.

contacts are mainly with corporate security officers. Key messages can be further disseminated through existing Corporate and government systems, thereby increasing the potential audience to over 1 million people.

AMERICAN PUBLIC

Delivery Systems: EAS, The Media, public government agency websites.

EAS: Emergency Alerting System.¹⁹

Coverage: Nationwide, via television and radio media.

Information capability: Unclassified.

System Administrator: FEMA, via Presidential authority.

Miscellaneous information: The FEMA Operations Center is the activation and termination point for the national-level Emergency Alerting System (EAS). This system consists of a voluntary nationwide network of common carriers, radio and television networks and stations (audio only), cable networks and systems, and wire services. These stations are issued EAS authorization by the Federal Communications Commission (FCC). The system is designed to maintain communications with the general public in the event of an attack, a threat of war, a state of public peril, disaster, or other national emergency. Each EAS station assumes the responsibility for disseminating to a specifically designated area with Presidential messages, Governor's messages, state and local information, and national programming and news in addition to its normal programming. The activation of the EAS can be preceded by an announcement over the NAWAS for all warning points to ensure their televisions/radios are turned on. Currently, this system can ONLY be activated by direction of the President. When appropriate and approved by the President, the EAS may be activated by the FOC to disseminate announcements via radio and television media. Once activated by the FOC, under direction of the President, ALL television and radio media circuits are "seized" and under complete control of the FOC until released back to normal operation.

The Media: Written, television, radio, Internet.

Coverage: National and worldwide.

Information capability: Unclassified.

System Administrator: The Attorney General, or proper designee.

Miscellaneous information: Live news conferences, with the simultaneous release of an appropriate written press release, is the preferred method of delivering threat information. This allows for a full explanation of the information as well as the opportunity for a question and

¹⁹ See Appendix S for EAS/ FCC document.

answer discourse, if desired. The purpose of a live news conference is the release of terrorist threat information in a timely fashion to the largest audience possible.

Websites: Internet Service Providers, Email

Coverage: National and worldwide.

Information capability: Unclassified.

System Administrator: Various government agencies.

Miscellaneous information: Each Federal, State and Local government agency should be encouraged to post current threat information, which has been released, to the general public via an authorized press release, on their public websites.

NOAA / NWR: National Oceanic and Atmospheric Administration / National Weather Radio.²⁰

Coverage: National

Information capability: Unclassified.

System Administrator: United States Department of Commerce, National Oceanic and Atmospheric Administration.

Miscellaneous information: NOAA Weather Radio (NWR) broadcasts National Weather Service warnings, watches, forecasts and other hazard information 24 hours a day. NWR and the Emergency Alerting System (EAS) use the same digital protocols, and NWR is the primary means for National Weather Service alerts to activate the EAS. Weather radios equipped with a special alarm tone feature can sound an alert and give immediate information about a life-threatening situation. The hearing and visually-impaired also can get these warnings by connecting weather radios with alarm tones to other kinds of alerting devices such as strobe lights, pagers, bed-shakers, personal computers and text printers.

These systems represent what is currently available for use by the Homeland Security Advisory System. There are on-going, short term projects which will enhance the system in the very near future. A prime example is the acquisition and implementation of software which will allow LEO a "push" capability, as opposed to its current "pull" capability. This additional software will allow LEO to send instant alerts to predetermined users who are on-line. If the recipients fail to acknowledge receipt of the alert within a predetermined period of time (i.e. five or ten minutes), the system will contact the recipient via alpha-numeric pager, cell phone, or wireless Personal Digital Assistant (PDA), with a text message advising that an alert has been issued via LEO. In addition, LEO is exploring ways in which to place its services in every law enforcement dispatch center across the United States on a dedicated computer terminal, in order

²⁰ See Appendix T for NOAA document.

to ensure 24 hour a day, seven days a week coverage. This will make the software alerting system even more valuable in terms of alerting all Federal, State and local law enforcement.

CHAPTER V

REPORT OF 45-DAY COMMENT PERIOD

HSPD-3 required the Attorney General, in coordination with the Assistant to the President for Homeland Security, to seek the views of government officials at all levels and of public interest groups and the private sector on the proposed HSAS. The public comment period was opened 45 days from the date of March 11, 2002. There were two primary mechanisms set in place to help generate responses from the intended audiences. The first involved the establishment of an HSAS comments website at hsascomments@fbi.gov.²¹ The second mechanism involved the preparation of an electronic communication sent to all FBI field offices around the country requesting that the FBI make contact with State and local government officials, emergency managers, State and local law enforcement officers, firefighters, emergency medical technicians, 911 dispatchers, emergency room department heads, hospital administrators, public health laboratories, relevant private industry leaders, and any other personnel involved with emergency response. The following summaries are the results of this 45-day comment period:

Public Opinion of HSAS Concept

The responses from the target audiences were overwhelmingly in favor of the concept of a national advisory system to provide notification of terrorist threats within the United States. Out of 599 relevant responses from both the FBI Field Office surveys and HSAS website, **96% (575)** were for and **4% (24)** against an alert system.²²

Findings of HSAS Comments Website²³

During the 45 day public comment period, 751 e-mails and written responses were received as a result of the HSAS comments website. Of the 751 e-mails and written responses, 511 (68%) contained comments of relevance to the development of the HSAS. The remaining 240 (32%) responses were deemed not relative to the development of the HSAS.

A review of the 511 relevant responses determined that: 240 (47%) had been sent by “private individuals, ” 155 (30%) had been sent by “government officials at all levels,” 105 (21%) had been sent by the “private sector” and 11 (2%) had been sent by “public interest groups”.

Listed below are the major themes that emerged from the analysis and the number of relevant comments. It should be noted that the total number of relevant comments (652) exceeds

21 See Appendix U for copy of HSAS Comments Web page.

22 See Appendix C, “ Response to the Development of a Homeland Security Advisory System” graph.

23 See Appendix V for entire Report of Findings of HSAS Comments Website.

the total number of responses (511) due to some respondents making multiple relevant comments.

• alert status	221	(34%)
• color coding/color schemes	132	(20%)
• basic design	135	(21%)
• other	92	(14%)
• service	72	(11%)
Total relevant comments	<u>652</u>	<u>100%</u>

After responses were reviewed, and major themes (alert status, color coding/color scheme, basic design, service and other) identified, analysts summarized the comments within each major theme to illustrate more specifically the observations of the respondents.

The number of responses for a major theme and the number of comments made by respondents for that theme may not be equal. This is due to some respondents making multiple comments in their responses.

Alert Status: There were 221 responses that included references to “alert status” issues. The following observations were provided by respondents:

- 200 (90%) respondents indicated that they wanted to be notified of the current threat level (as of the day of their response) and wanted to know in what manner they would be notified.
- 127 (57%) respondents suggested that the alert status could be provided through a website,
- 70 (32%) respondents wanted to know in what manner the public will be alerted of the threat level,
- 47 (21%) respondents suggested that the alert status could be delivered using the television (scrolling message, color dot in the corner of the screen, etc.),
- 20 (9%) respondents suggested that the alert status could be delivered by displaying a symbol of the threat status at local government facilities,
- 6 (3%) respondents indicated that the alert status could be delivered by placing a symbol for the threat status at the top of newspapers.

Color Coding/Color Scheme: There were 132 responses regarding "color coding/color scheme." The following observations were gathered from analyzing the comments:

- 78 (59%) respondents indicated that other colors should be used because the colors used did not follow the color spectrum,
- 23 (17%) respondents said that color blind people would not be able to identify the colors,
- 18 (14%) respondents observed that the military already has a system in place to alert the public of a threat (Alpha, Bravo, Charlie, Delta), and
- 6 (5%) respondents suggested there should be corresponding numbers or

letters along with the colors.

Basic Design: There were 135 responses regarding “basic design.” The following information resulted from analyzing the comments:

- 73 (54%) respondents wanted to know what guidelines to follow when a threat level is assigned,
- 43 (32%) respondents indicated that the threat warnings should be regionalized,
- 10 (7%) respondents indicated that the HSAS should be similar to the weather advisories, and
- 7 (5%) respondents suggested that the HSAS should be similar to the military advisories (Alpha, Bravo, Charlie, Delta).

Service: There were 72 responses regarding “service.” The following categories of comments characterize the responses in the “service” area.

- 20 (28%) companies offered to provide services regarding delivering alert messages to the public and/or delivering alert messages to federal, state and local governments,
- 15 (21%) respondents asked questions regarding the implications for 911 services when alerts are disbursed,
- 12 (17%) individuals were looking for employment, and
- 37 (51%) were other companies/individuals/groups wanting to provide HSAS related services other than services for delivering alert messages.

Other: There were 92 relevant responses that did not fall into the four predominant themes listed above. The following are indicative of the types of comments in the “other” area.

- 38 (41%) respondents provided ideas regarding the HSAS (distributing laminated cards with the threat levels and providing a terrorist awareness guide),
- 17 (18%) respondents indicated that the federal, state and local governments will need funds to support the HSAS initiative,
- 10 (11%) respondents talked about Immigration and Naturalization Services (INS) related issues (borders, immigrants, visas), and
- 10 (11%) respondents indicated that training for local, state, and government agencies is needed to support the HSAS.

FBI Field Office Surveys

A Field Survey was sent out to all FBI Field Offices on April 4, 2002 to notify respective audiences and receive feedback on the Homeland Security Advisory System by May 1, 2002. Target audiences contacted, included State and Local government officials, emergency managers, state and local law enforcement officers, fire fighters, emergency medical technicians,

911 dispatchers, emergency room department heads, hospital administrators, public health laboratories, relevant private industry leaders, State Adjutant Generals, and any other personnel involved with emergency response.

Other suggested organizations notified, provided they had chapters in the Field Office Territories, included: International Association Chiefs of Police, National Sheriffs Association, Major City Chiefs, Major County Sheriffs, Police Executive Review Forum, National Organization of Black Law Enforcement Executives, Fraternal Order of Police, International Brotherhood of Police, International Union of Police, National Association of Police Organizations, National Troopers Coalition, National Emergency Managers Association, International Association of Fire Chiefs, International Association of Fire Fighters, American Association, US Conference of Mayors, National League of Cities, National Association of Counties, National Conference of State Legislatures, Council of State Governments, International Association of City/County Managers, American Legislative Exchange Council, National Association of Attorneys General, and the National District Attorneys Association.

After reviewing all Field Office survey responses, it was determined that 643 were directly relevant to the HSAS. All relevant responses were broken down into the following five major themes:²⁴

- Threat Alert Notification
- Basic Design (Structure/Color)
- Proposed Dissemination Services
- Suggestions
- Questions and Concerns

The prevalent responses for each theme are noted below. Refer to the supporting graphs for additional theme information.

Threat Alert Notification Theme:

- 61 (17.5%) respondents thought that a current Threat Alert should be disseminated via phone (satellite & wireless) / Alpha-Numeric Pager / PDA's / FAX,
- 42 (12.0%) respondents felt that using an E-mail Blast would be effective.

Basic Design Theme:

Structure:

- 34 (35.8%) of the respondents thought there should only be 3 or 4 levels on the advisory system, making it easier to remember the associated threat risks.

Colors:

²⁴ See Appendix C for corresponding graphs.

- 13 (46.4%) of the respondents wanted to eliminate the color green. They felt that our country would never utilize this color again.

Proposed Dissemination Services Theme:

- 6 (37.5%) respondents felt that a National Hotline or 1-800 number / National Information Center should be established to provide current Threat Conditions (possibly at state level).
- 4 (25.0%) respondents felt that quick reference cards/posters should be available for wide distribution to 911 dispatchers, police, fire, and all local, state and federal agencies.

It is recommended that periodic testing of the HSAS be conducted to ensure the inclusiveness and effectiveness of information dissemination techniques to a multitude of agencies and departments.

Suggestions Theme:

- 31 (63.3%) respondents felt that training sessions and educational programs should be established and made available for all public, private, and law enforcement groups. These same comments also suggested that detailed guidance should be provided to agencies (local/State/Federal) with regards to what is expected of them when responding to a particular threat alert and providing clear definitions/examples of each of the HSAS levels.
- 8 (16.3%) felt that periodic announcements of the current threat status with a Date/Time Group and clear definition of the specific threat (type of Assault/Weaponry) should be made to the local, State and Federal agencies.

It is recommended that HSAS education and training initiatives be developed for State and local government agencies and departments to promote the HSPD-3 objectives of information communication and collaborative response and recovery efforts. It is also recommended that education and awareness programs be developed at the national level to inform private industry and the American public of HSAS responsibilities.

Questions and Concerns Theme:

- 27 (25.5%) respondents felt that all levels of government, Federal, State and local, should use one standardized rating/warning system. A standardized system would allow a common vernacular to be created throughout all agencies, departments, and levels of government, reducing the possibility of confusion (For Example: DOD, GSA, FEMA, and OHS on one system).
- 25 (23.6%) felt a formal notification of the Current Threat Alert status and some direction should be given to the Emergency Management Community and other Non-Law Enforcement agencies prior to the public being notified.

- 22 (20.8%) felt there should be regional threat alert, not a National one. Law enforcement needs to know detailed information to defend the population from threats in an effective and efficient manner, reducing the threat area where appropriate.

It is recommended that dedicated federal grant programs be identified and made available to State and local governments for law enforcement and emergency responder initiatives that promote HSAS objectives.

CHAPTER VI KEEPING AMERICA INFORMED

As this document is being prepared and submitted, several major prevention and preparedness initiatives are underway to help reduce the potential for another terrorist attack.

Critical to any new initiatives is the necessity to coordinate and communicate intelligence to all involved in the vigilant efforts to keep the United States safe from terrorist atrocities. Most importantly, the American public must be kept informed of the known and evaluated Threat Conditions, through the combined efforts of Federal, State, local and private information networks. Furthermore, the Federal, State and local governments must devote dedicated resources to developing, practicing, updating and maintaining Protective Measures and contingency action plans in order to avert, respond to and recover from terrorist events in the most effective and expeditious manner possible.

To this end, this report recommends the following in support of HSDP-3 objectives:

It is recommended that:

- ◆ **this report serve as the complete written recommendations by the Attorney General of the United States to the President for proposed refinements to the Homeland Security Advisory System as directed in HSPD-3.**
- ◆ **legislation establishing the Department of Homeland Security include language that requires the Attorney General of the United States be consulted in the assignment of future Threat Conditions.**
- ◆ **the HSAS serve as the national framework for State and local government agencies and private industry, and that the OHS encourage these organizations to emulate the HSAS, making further enhancements as needed to meet specific community and business requirements.**
- ◆ **whenever Threat Conditions are posted, the condition be clearly indicated with both the color-coding and risk description.**
- ◆ **the American public and private industry be encouraged to utilize the HSAS, and American Red Cross publications to facilitate the development of Protective Measures for their own specific requirements.**
- ◆ **all HSAS education and awareness programs emphasize that despite the best decision to assign an appropriate Threat Condition, there can be no guarantee that a terrorist attack will be prevented.**
- ◆ **all current information dissemination systems identified in this report be adopted as those that will be utilized to disseminate threat information as**

called for under HSPD-3. These systems should be utilized until such time that a more permanent and all-inclusive system is perfected by which threat information will be disseminated community and nation wide.

- ◆ **periodic testing of the HSAS be conducted to ensure the inclusiveness and effectiveness of information dissemination techniques to a multitude of agencies and departments.**
- ◆ **HSAS education and training initiatives be developed for State and local government agencies and departments to promote the HSPD-3 objectives of information communication and collaborative response and recovery efforts.**
- ◆ **education and awareness programs be developed at the national level to inform private industry and the American public of HSAS responsibilities.**
- ◆ **dedicated federal grant programs be identified and made available to State and local governments for law enforcement and emergency responder initiatives that promote HSAS objectives.**

While there can be no guarantee that any single system can prevent a future terrorist attempt, the concerted efforts of Federal, State and local governments, along with private industry and the American people will send a resounding message to the world; We are prepared and we will remain strong.

TABLE OF APPENDICES

- Appendix A: Executive Order 13228 Establishing Office of Homeland Security
- Appendix B: Homeland Security Presidential Directive-3
- Appendix C: FBI Field Office Survey Graphs
- Appendix D: List of American Red Cross Materials
- Appendix E: American Red Cross Homeland Security Advisory System Recommendations
- Appendix F: American Red Cross brochure "*Terrorism: Preparing for the Unexpected*"
- Appendix G: National Threat Warning System document
- Appendix H: AUTODIN and DMS document
- Appendix I: WAWAS Members
- Appendix J: NLETS document
- Appendix K: NLETS Regional Members
- Appendix L: RISS document
- Appendix M: LEO document
- Appendix N: NAWAS Regional Members
- Appendix O: InfraGard document
- Appendix P: ISAC document
- Appendix Q: CERT/CC document
- Appendix R: ANSIR document
- Appendix S: EAS / FCC document
- Appendix T: NOAA document
- Appendix U: Copy of hsascomments@fbi.gov web page for 45-Day Comment Period
- Appendix V: Report of Findings of HSAS Comments Website