FADED COLORS: FROM THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS) TO THE NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)

Sharp, Vincent H.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FADED COLORS: FROM THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS) TO THE NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)

by

Vincent H. Sharp

March 2013

Thesis Advisor: Robert Simeral
Second Reader: John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE FADED COLORS: FROM THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS) TO THE NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Vincent H. Sharp			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

After the events of 9/11, Homeland Security Presidential Directive-3 (HSPD-3) established the 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 the American people. Under HSAS, threat levels were raised or lowered 16 times, but never below Threat Level Yellow (Elevated Condition). HSAS should have been straightforward and easy to understand. What evolved was confusion over alerts, lack of specific threat information, concerns over costs to institute and maintain protective measures, and questions regarding what was expected of citizens. Government agencies, the private sector, and the general population became immune with the threat level remaining at or above Yellow.

HSAS was woefully misunderstood not just by the general population, but also within federal, state, and local governments. Ridiculed by comedians, HSAS gradually began to disappear, to the point where it was necessary to search to find the current threat level, whereas it had once been prominently posted. The purpose of this thesis is to review HSAS and the associated problems, look at comparable international systems, and present an alternative recommendation to provide timely and informative warnings of terrorist threats, and restore credibility by merging HSAS with the already existing DoD force protection conditions.

14. SUBJECT TERMS Homeland, Security, Advisory, System, National, Terrorism, Threat, Alert, Terrorist, Warnings			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FADED COLORS: FROM THE HOMELAND SECURITY ADVISORY SYSTEM (HSAS) TO THE NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)

Vincent H. Sharp
Operations Evaluation Analyst, ARNORTH/Civil
Support Readiness Group-West, San Antonio, Texas
B.S., United States Air Force Academy, 1977
M.S., University of Arkansas, 1987

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2013**

Author: Vincent H. Sharp

Approved by: Robert Simeral
Thesis Advisor

John Rollins
Second Reader

Harold A. Trinkunas, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

After the events of 9/11, Homeland Security Presidential Directive-3 (HSPD-3) established the 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 the American people. Under HSAS, threat levels were raised or lowered 16 times, but never below Threat Level Yellow (Elevated Condition). HSAS should have been straightforward and easy to understand. What evolved was confusion over alerts, lack of specific threat information, concerns over costs to institute and maintain protective measures, and questions regarding what was expected of citizens. Government agencies, the private sector, and the general population became immune with the threat level remaining at or above Yellow.

HSAS was woefully misunderstood not just by the general population, but also within federal, state, and local governments. Ridiculed by comedians, HSAS gradually began to disappear, to the point where it was necessary to search to find the current threat level, whereas it had once been prominently posted. The purpose of this thesis is to review HSAS and the associated problems, look at comparable international systems, and present an alternative recommendation to provide timely and informative warnings of terrorist threats, and restore credibility by merging HSAS with the already existing DoD Force Protection Conditions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CDEM	Colorado Division of Emergency Management
CHDS	Center for Homeland Defense and Security
CIPAG	Critical Infrastructure Protection Advisory Group
CIPWG	Critical Infrastructure Protection Working Group
CRS	Congressional Research Service
DHS	Department of Homeland Security
DoD	Department of Defense
DTN	Terrorist Threat Assessment Netherlands
EMD	Emergency Management Division
FBI	Federal Bureau of Investigation
FPCON	Force Protection Conditions
GAO	General Accounting Office
HSAS	Homeland Security Advisory System
HSEMD	Homeland Security and Emergency Management
HSPD	Homeland Security Presidential Directive
NCTb	National Coordinator for Counterterrorism
NCTC	Counter-Terrorism Committee
NCTP	National Counter Terrorism Plan
NERC	North American Electric Reliability Council
NTAC	National Threat Assessment Centre
NTAS	National Terrorism Advisory System
UK	United Kingdom
USNORTHCOM	United States Northern Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The research and writing of this thesis has been a very intensive period for me, and for reasons far beyond writer's block, have led to numerous delays in completion, as well as many discoveries about myself in the process. I would like to acknowledge the staff and professors of the Center for Homeland Defense and Security who have established and are maintaining an exceptional program related to the security of our homeland, a subject to which I have devoted almost 40 years and hope to continue for several more. I appreciate the thought provoking discussions and the patience to allow me to work through my personal struggle.

To the members of Class 0703–0704 (the Potato-Heads), of which I have many memories from our time spent in Shepherdstown, your status will always remain special and equal to that reserved for those I have served with for your support in keeping me going through a dark time in my life. While I may not remain in close contact, I think of you often and look forward to reading of your future achievements.

To my family, I owe the largest debt for giving up precious time with me to pursue this program and supporting me when I could have just as easily walked away. To Sue, my wife and closest friend, I owe untold gratitude, not only for supporting me to accomplish this goal, but for all she has done throughout my career. To Bob and Melissa, thanks for understanding when I was not there to help with your school project/event, missed a birthday/holiday, or the multitude of other events in your lives that were just as important. I hope you know how much I missed not being there. And finally to Tony, we all miss you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In April 2011, the United States moved from a color-coded Homeland Security Advisory System (HSAS), which had been in place for nine years, to a new National Terrorism Advisory System (NTAS), which has yet to issue its first alert. This thesis examines how a homeland security alert system should function to keep citizens aware of threats to the public and why the system was changed. It also discusses and recommends a proposal to merge or replace the current system with the Department of Defense Force Protection Conditions (DoD FPCON).

On March 12, 2002, six months after the attacks on the Pentagon and World Trade Center, President Bush signed Homeland Security Presidential Directive-3 (HSPD-3) and created HSAS. Governor Tom Ridge then introduced the system and described how it worked. In his remarks, Governor Ridge elaborated that the system had the following features.

- Designed to measure and evaluate terrorist threats
- Communicate threats to the public in a timely manner
- Flexible to apply to threats made against a city, a state, a sector, or an industry
- Provides a common vocabulary
- Provides clear, easy to understand factors that help measure threat
- Empowers government and citizens to take actions to address the threat

HSAS had five levels, with recommended protective measures, to represent an increasing level of terrorist threat. While binding on the executive branch, HSAS was voluntary to other levels of government and the private sector. Assigned threat conditions were reviewed at regular intervals to determine whether adjustments were warranted (Bush, 2002).

Despite these assurances, in the nine years HSAS existed, the country remained at Threat Level Yellow (Elevated Condition) or higher with the last change in alert levels

having occurred in August 2006. The two lowest levels were never used (Homeland Security, 2008a). Confusion occurred over what state and local governments were required to do when a change was directed. Private citizens received misleading information that led to an increasing tendency to dismiss the advisory system.

On July 14, 2009, Department of Homeland Security (DHS) Secretary Janet Napolitano established the Homeland Security Advisory System Task Force to conduct a 60-day review of HSAS. Its mission was to assess the effectiveness of the system in informing the public and communicating protective measures concerning terrorist threats and report back to the Secretary with its findings (Homeland Security, 2009a).

When the task force completed its review, Secretary Napolitano announced on January 27, 2011 that over the next 90 days, HSAS would be replaced in favor of NTAS. Secretary Napolitano expressed that NTAS would more effectively communicate information about terrorist threats by providing timely, detailed information to the public. The color-coded system would be replaced by alerts clearly stating that an "imminent or elevated threat" existed along with a concise summary of the threat, information about actions being taken to ensure public safety, and recommended steps individuals, communities, businesses, and governments could take (Homeland Security, 2011e). On April 20, 2011, Secretary Napolitano announced implementation of NTAS, a robust terrorism advisory system replacing the color-coded system (Homeland Security, 2011d).

B. RESEARCH QUESTION

HSAS should have been a straightforward and easy to understand system to alert government agencies, the private sector, and civilians to increased threats of terrorist activity. However, what evolved was confusion over alerts, a lack of specific information being shared as to the nature of the threats, concern over the additional costs to institute and maintain protective measures over a long period, and questions from citizens regarding what was expected of them. HSAS was widely criticized at multiple levels and had definite flaws that required repair to restore confidence and credibility to provide timely and informative warnings of terrorist threats. The question is how, could, or

should HSAS be revised to provide federal, state, and local governments, private organizations, and ordinary citizens with timely and informative warnings of terrorist threats?

C. SIGNIFICANCE OF RESEARCH

This thesis reviews HSAS, associated international systems, and the identified flaws that have now led to the introduction of NTAS. Much of the debate about HSAS pertained to the lack of information forthcoming from the government about the nature of terrorist threats and where they may strike. The economic and psychological factors of maintaining high levels of sustained alert over a long period of time were also concerns along with the lack of specific measures to take when a threat level was changed. This thesis also explores an alternative system already in place within the Department of Defense (DoD). The Department of Defense Force Protection Conditions (DoD FPCON) would provide a quick and easy method to restore credibility and make notification of terrorist threats a viable and easily understood system. Additionally, since NTAS has been in place for over 18 months, an initial assessment can be made as to how effective it has been in replacing HSAS. However, as no NTAS alerts have been issued during this time, no metrics are available to measure its effectiveness. The federal government, state and local governments, private industry and the American public are the consumers of this research.

D. ARGUMENT

Under HSAS, the author would arrive at his office on Fort Sam Houston, after passing through an entry gate and showing his identification card to a security guard, and enter the world of FPCON Alpha, which is defined as an increased general threat of possible terrorist activity against personnel or facilities, the nature, and extent of which are unpredictable (Air Force Manual 10-100, 2004, p. 19). Since DoD installations were exempt from following HSAS, he could now, in theory, relax his vigilance as he was no longer “in” San Antonio, and therefore, subject to Threat Level Yellow (Elevated Condition), which is defined as a significant risk of terrorist attacks (Bush, 2002). By definition, in just passing through a gate and showing his identification, the author

transitioned from a significant risk of terrorist attack down to an increased general threat. Upon departing Fort Sam Houston and the protection of FPCON Alpha, he would reenter the elevated threat area within San Antonio and make the drive to the San Antonio airport where upon entering the terminal, he would be greeted with the following recorded announcement: “The Department of Homeland Security has changed the threat level to Orange.” No mention was made that this change was designated only for the aviation sector or that it had remained at that level since it was raised in August 2006 (Chertoff, 2006). With Threat Level Orange being defined as a high risk of terrorist attack, in the space of five miles and less than 15 minutes, the author had traveled from a general threat (FPCON Alpha) through a significant risk (Threat Level Yellow) to a high risk (Threat Level Orange) of a terrorist attack (Bush, 2002). Psychologically, this continuous change to unknown threats was more extreme than having been stationed in Riyadh, Saudi Arabia during Desert Storm under the threat of Scud attacks. The Scuds were real, the threat levels were constant, and thus, it was possible to adapt his living situation accordingly. However, in this situation, what choices were available: live and react to the high-risk threats, ignore the high risk and take a more middle of the road response with the significant risk, or ignore the risk completely? Without specific threat information with which to assess the situation, the choice was either be controlled by the threat of a terror attack or maintain a relatively normal lifestyle, take the appropriate precautions, and rely on law enforcement and intelligence agencies to provide the necessary information at the appropriate time.

The introduction of NTAS promised to provide better and timelier information, and therefore, should have removed any confusion while making the risk decision process simpler. However, the author still finds himself going from a higher to a lower risk when entering Fort Sam Houston. Also, the disappearance of Threat Level Orange signs and audio alerts is primarily the only difference seen at airports.

HSPD-3 opened with the statement that the nation requires a 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. Such a system would provide warnings in the form of a set of graduated “threat conditions” that

would increase as the risk of the threat increases (Bush, 2002). HSAS did provide citizens with information to provide security and protection from terrorist attack, but was itself under attack due to the timeliness or lasting effects of vague warnings that provided little information on the true nature of the threats. No major terrorist attacks occurred following implementation of HSAS, but that did not mean HSAS provided the best response. In reality, the long periods of time before lowering the threat levels or not providing the public with complete explanations worked in the terrorist's favor as it increased both the financial burden on cities and kept citizens in constant fear of additional attacks.

This argument began with a comparison of HSAS and FPCON systems with a specific purpose in mind. It is the author's hypothesis that HSAS and FPCON had the same goal, essentially the same terminology, were based on the same intelligence, and could have been merged or linked to create an alternative advisory system that would have been easier to understand and implement. Advantages of introducing FPCON as an alternative system would include a consistent level of threat, specific response measures, warnings issued on a regional or local basis depending on the threat, and a system with which a large portion of the federal government and general population was already familiar.

The introduction of NTAS has not changed the argument. The very fact that NTAS has not issued any alerts over its initial 20 plus months while reports of law enforcement thwarting terrorist attacks are received, intelligence agencies are providing information of potential attacks, and/or minor attacks are being executed, creates concern about the new system.

E. METHOD

An analysis of the documented flaws with HSAS and a sample case study is the method used to validate this thesis. Having indicated the areas in which the system is currently broken and with the knowledge that the system required revision if it was to remain a credible and useful tool, a recommendation is then proposed and a description provided of how to eliminate current flaws. The recommendation describes how a merger

of HSAS with FPCON would provide one credible and recognizable viable system. NTAS is also reviewed as the replacement for HSAS to ascertain if in fact it has measured up to its stated goals.

II. LITERATURE REVIEW

With establishment of HSAS (Bush, 2002), the United States entered a new era in fighting terrorism. As opposed to the Cold War era of nuclear weapons with air raid shelters accompanied by duck and cover drills, HSAS was designed to provide the nation with an easy means to disseminate information to federal, state, and local authorities and the American people (Bush, 2002). For nine years, the system in place was misunderstood, ridiculed, ignored, and it was not completely clear what level was in effect, what the threat was, or what the general public should have been doing. Starting with a general background of HSAS as established by White House and Homeland Security documents, this research then turned to terrorist advisory systems used by other countries to determine if aspects could be incorporated into HSAS. The author expanded his search for outside sources and researchers with views on HSAS and its effectiveness. Next, he did a search of state homeland security websites and concluded the initial review by evaluating DoD FPCON.

A. HOMELAND SECURITY ADVISORY SYSTEM

Governor Tom Ridge introduced HSAS on March 12, 2002 and elaborated on the following features (White House, 2002a).

- Designed to measure and evaluate terrorist threats
- Communicate threats to the public in a timely manner
- Flexible to apply to threats made against a city, a state, a sector, or an industry
- Provides a common vocabulary
- Provides clear, easy to understand factors that help measure threat
- Empowers government and citizens to take actions to address the threat

Governor Ridge continued to describe the five color-coded levels that were at the core of the advisory system, by stating, “The nation currently stands in the yellow condition, in elevated risk….we will not be able to lower the condition to green until, as the President said yesterday, the terror networks of global reach have been defeated and

dismantled" (White House, 2002a). Associated with each level were recommended protective measures to be taken; however, the measures were very generic and the actual development of appropriate measures was left to each federal agency (Bush, 2002). A key point is that HSAS was only binding on the executive branch and suggested to other levels of government and the public/private sector (Bush, 2002). When initially designed, the advisory system did not provide any measures for states, local communities, industry, or private citizens. How this situation was remedied to some degree is discussed in a following section. The five levels contained within the advisory system were the following (Bush, 2002):

- **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Refining and exercising as appropriate preplanned protective measures;
    - Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
    - Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
- **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks.
    - Checking communications with designated emergency response or command locations;
    - Reviewing and updating emergency response procedures; and
    - Providing the public with any information that would strengthen its ability to act appropriately.
- **Elevated Condition (Yellow)**. An elevated condition is declared when there is a significant risk of terrorist attacks.
    - Increasing surveillance of critical locations;
    - Coordinating emergency plans as appropriate with nearby jurisdictions;
    - Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
    - Implementing, as appropriate, contingency and emergency response plans.

- **High Condition (Orange)**. A high condition is declared when there is a high risk of terrorist attacks.
    - Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
    - Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
    - Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
    - Restricting threatened facility access to essential personnel only.
- **Severe Condition (Red)**. A severe condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a severe condition are not intended to be sustained for substantial periods of time.
    - Increasing or redirecting personnel to address critical emergency needs;
    - Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
    - Monitoring, redirecting, or constraining transportation systems; and
    - Closing public and government facilities.

Figure 1. Homeland Security Advisory System (From: Homeland Security, 2008b)

The decision to raise or lower the threat level was initially given to the Attorney General and was based on gathered intelligence and the associated risk. Factors used for analyzing threat assessments before recommending a change to the alert level included the following (Bush, 2002).

- 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?

Authority to assign threat conditions was transferred from the Attorney General to the Secretary of Homeland Security on February 28, 2003 with the signing of Homeland Security Presidential Directive-5 (Bush, 2003). The Secretary consulted with the Homeland Security Council prior to raising or lowering the threat (Reese, 2003).

The remainder of the White House and Homeland Security documents revolve around the raising and lowering of the threat level over the years and the rationale or intelligence behind making the decision. Since its inception, the threat level was raised or lowered 16 times (Homeland Security, 2008a) beginning with the first anniversary of the 9/11 attacks on September 10, 2002 (White House, 2002b). The latest was the announcement that the aviation sector was being lowered from red to orange for inbound flights from the United Kingdom (UK) on August 13, 2006 (Homeland Security Press Release, 2006).

B. INTERNATIONAL ADVISORY SYSTEMS

The next set of literature reviewed concerned international terrorist alert or advisory systems. The primary reason for evaluating systems in other countries is that their struggle against terrorism has been going on for much longer. As a result, these systems have been in place for some time. An interesting observation is that despite the worldwide nature of the terrorist threat, only a limited number of countries have actually established a threat advisory system. Surprisingly, no two European anti-terror alert systems are the same despite the proximity and open borders. Each country decides when and how to activate a given alert level within its territory. The Home Secretaries of the

United Kingdom and Spain did meet in an attempt to create an alert system for the entire European Union; however, a solution has yet to be reached (Sordo, 2006). Despite not developing a common alert system, European Union members have established a common definition of terrorism along with common penalties for terrorist crimes (Archick, Ek, Gallis, Miko, & Woehrel, 2006, p. 13).

1. France

The French system, Vigipirate, was designed in 1978 and consists of two levels, "simple" and "reinforced" above normal, which was changed to a four-level color-coded system in 2003 to make the system more flexible and understandable (Intellnet, 2003). Threats are assessed based on national and international circumstances and proposed changes to the alert level are presented to the President and to the Prime Minister, who have the authority to trigger "Plan Vigipirate." The appropriate authorities including national and local government agencies then implement the relevant monitoring, prevention and protection measures (Absolute Astronomy, 2008).

A defining feature of Vigipirate is the specificity of response measures corresponding to the various threat levels, which is tied to specific sectors. Also notable is the openly public release of measures to be taken in the event of plan activation. Public engagement and confidence in the system is likely to be much higher under a system that releases, rather than shields, threat level information. Vigipirate relies on joint participation and advances the principle of shared responsibility from individual citizens to government agencies (Absolute Astronomy, 2008).

Levels of alert for “Plan Vigipirate”
Yellow level—to stress vigilance
Raise security levels to face real yet still uncertain dangers, through measures that are local and minimally disruptive of normal activity, while preparing to switch to “orange” or “red” within a few days.
Orange level—to warn of terrorist action
Take measures against plausible risks of terrorist action, including the use of means that are moderately disruptive to normal public activities, while preparing to switch to “red” or “crimson” on short notice where possible.
Red level—to warn of serious attempts
Take measures against a proven risk of one or more terrorist actions, including measures to protect public institutions and putting in place appropriate means for rescue and response, authorizing a significant level of disruption to social and economic activity.
Crimson level—to warn of major attempts
Notification of a risk of major attacks, simultaneous or otherwise, using non-conventional means and causing major devastation; preparing appropriate means of rescue and response, measures that are highly disruptive to public life are authorized.

Figure 2. Vigipirate (From: “Vigipirate,” 2008)

2. United Kingdom

The United Kingdom had a threat system in place for years; however, details and warnings were kept from public scrutiny until 2006 following the London subway bombings. The British system consists of five threat levels, is now color-coded, and is based on the assessment of a range of factors including current intelligence, recent events, and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response are made with this in mind. The British system also includes three response levels, which provide an indication of the security measures that should be applied (Security Service Security Service MI5, 2008).

Threat level		Response	
Critical	an attack is expected imminently	**EXCEPTIONAL**	Maximum protective security measures to meet specific threats and to minimize vulnerability and risk
Severe	an attack is highly likely	**HEIGHTENED**	Additional and sustainable protective security measures reflecting the broad nature the threat combined with specific business and geographical vulnerabilities and judgments on acceptable risk
Substantial	an attack is a strong possibility		
Moderate	an attack is possible, but not likely	**NORMAL**	Routine protective security measures appropriate to the business concerned
Low	an attack is unlikely		

Figure 3. UK Threat Advisory System (From: UK Intelligence Community Online, 2008)

3. Netherlands

The Netherlands have a unique system that in reality is two separate systems that work together as one to provide terror alerts. The National Coordinator regulates the entire system for Counterterrorism (NCTb) and the Minister of Justice announces any changes. The task of the NCTb is to minimize the risk of terrorist attacks in the Netherlands and take prior measures to limit the potential impact of terrorist acts. The NCTb is responsible for the central coordination of counterterrorism efforts and ensures that cooperation between the parties involved is and remains of a high standard (National Coordinator for Counterterrorism (NCTb), 2008).

The Terrorist Threat Assessment Netherlands (DTN) determines the general threat level for the Netherlands and Dutch interests abroad based on a wide range of intelligence (National Coordinator for Counterterrorism (NCTb), 2008). DTN consists of four levels: minimal, limited, substantial, and critical and are regarded as a threat range (National Coordinator for Counterterrorism (National Coordinator for Counterterrorism (NCTb), 2008). DTN does not deal with specific locations or times but with the question of how great is the risk that a terrorist attack will be carried out against the Netherlands? Since the assessment is so general, no security measures are taken based on DTN alone. It therefore primarily has an impact on the government's anti-terrorist policies (National Coordinator for Counterterrorism (NCTb), 2008).

Developed to look more specifically at the threat level within certain key areas or economic sectors, the Counterterrorism Alert System is not color-coded and is a special alert system for the government and the corporate sector. The alert system warns government services and businesses in the event of an increased level of threat so that they can quickly take security measures and distinguishes between four levels of threat (National Coordinator for Counterterrorism (NCTb), 2008). The NCTb supplies threat-related intelligence for the purposes of the system (National Coordinator for Counterterrorism (NCTb), 2008).

Intended for major economic sectors and local authorities with a focus on the country's critical infrastructure, the factors determining whether a sector becomes part of the system depends on the extent to which the sector is of vital financial and economic importance, whether the sector forms an attractive target for terrorist attacks, has the potential for terrorists to cause numerous casualties by unsophisticated means, or whether targets have a great symbolic value for Western society. The counterterrorism alert system currently covers 14 sectors: airports, railways, seaports, tunnels and flood defenses, chemical industry, oil industry, drinking water, electricity, natural gas, nuclear, municipal and regional transport, finance, public events, and hotels (National Coordinator for Counterterrorism (NCTb), 2008).

The Counterterrorism Alert System was not designed to communicate with the general public; however, if it becomes necessary to raise the threat level, the public will

be notified about the threat and the reasons behind raising the alert level. In the event of a terrorist threat, the system offers a standard ‘catalogue’ of measures per threat level and sector, the possibility of tailoring measures to the threat, the assurance that coordinated action is being taken by both private sector and the government, and nationwide coordination of security measures in both the technical and administrative sense. The system consists of four levels (National Coordinator for Counterterrorism (NCTb), 2008).

- **Standard**—Prudent precautions, normal operational management
- **Low**—Staff alerted, heightened degree of internal supervision, police surveillance
- **Moderate**—Security checks at points of entry, heightened police surveillance, certain processes stopped or re-routed
- **High**—Access to the facility blocked, evacuation, services discontinued, security checks by heavily armed personnel

The Counterterrorism Alert System considers threat information if the threat in question clearly relates to a participating sector. DTN, however, considers all threats pertaining to the Netherlands, which explains, for example, how DTN can indicate the general threat level is ‘substantial’ while the threat level for the participating sectors is basic because a threat to a specific sector does not necessary imply that the threat to the Netherlands as a whole has increased to the same degree.

	Terrorist Threat Assessment Netherlands (DTN)	Counterterrorism Alert System
For whom?	Politicians, policymakers, government bodies	Government and the sectors involved
Objective	To provide a general description of the potential threat to the Netherlands: what is the probability that a terrorist attack will take place in the Netherlands within a specific period? Informs the public about the general threat level.	To provide a description of the terrorist threat to a particular vital business sector. Intended to make it possible to take sector-specific measures in the event of a higher threat level.
Threat levels	• Minimal • Limited • Substantial • Critical	• Standard • Low threat • Moderate threat • High threat
Who or what is under threat?	The Netherlands as a whole (non-place-specific)	Participating sectors.
Measures	The DTN is too general to serve as a direct basis for security measures.	A package of measures (tailored to the threat level) is taken by both the sector in question and government.

Figure 4. DTN and Counterterrorism Alert System Comparison (From: National Coordinator for Counterterrorism (NCTb), 2008)

4. Australia

The Australian Government has a National Counter Terrorism Plan (NCTP) (National Counter-Terrorism Committee, 2005) that outlines the measures the country will take when intelligence indicates a potential threat. The current plan includes amendments to the alert system that took effect on October 1, 2008 (National Counter-Terrorism Committee, 2005). Changes to the threat level are issued at the discretion of the Prime Minister, Australian Government Attorney-General or other Australian Government Minister upon advice of the Counter-Terrorism Committee (NCTC), based on assessments of the threat environment by the National Threat Assessment Centre

(NTAC). The alert level informs national preparation and planning, dictates levels of precaution and vigilance to minimize the risk, and is used as the basis of public discussion of the risk to Australia. Each state and territory government determines its response to a terrorist incident based on an assessment of the risk (National Counter-Terrorism Committee, 2008).

As with all the systems, Australia relies upon strong intelligence to target prevention and preparedness measures based on risk management principles (National Counter-Terrorism Committee, Ch 3, para 13, 2005). NTAC issues threat assessments on which the various jurisdictions and agencies make risk management decisions on how best to respond to lower the risk (National Counter-Terrorism Committee, Ch 3, para 19, 2005). The Australian Counter-Terrorism Alert System is tiered and can be applied nationally, by jurisdiction, sector, or geographic location, and consists of four non-color-coded levels (National Counter-Terrorism Committee, Ch 3, para 20, 2005).

- **Low**—terrorist attack is not expected
- **Medium**—terrorist attack could occur
- **High**—terrorist attack is likely
- **Extreme**—terrorist attack is imminent or has occurred

Due to the tiered nature, security measures may vary across different jurisdictions or sectors (National Counter-Terrorism Committee, Ch 3, para 24, 2005).

5. Russia

Russia is the latest country to consider adopting a color-coded system and is planning to introduce one patterned after HSAS. Although discussed in the State Anti-Terror Committee for the last five years, it has yet to be introduced to the legislature (Bessonov, 2008).

6. Norway

While not having a nationwide threat advisory system, Norway's Police Security Service conducts and grades threat assessments into three levels: low, medium, or high. These assessments are then issued to the government agencies responsible for preventing and responding to threats. No protocol is in place to communicate directly with local

governments, the private sector, or the general public. Government agencies and county governors can be directed to take action; however, local governments, private sector, and the general public cannot be instructed to take actions unless warranted by law (General Accounting Office, 2004b, p. 47).

7. Germany

Germany also does not have a nationwide system of threat levels or requirements for specific actions to be taken. However, Germany does have a central communication center that processes information for forwarding to government agencies on actions to take during natural disasters and other threats. The communication center is responsible only for information management while the government agencies are responsible for deciding what measures to take. Threat information is communicated to the general public, individual institutions, and the business community by law enforcement agencies, state government, or federal government according to the nature of the threat (General Accounting Office, 2004b, pp. 47–48).

C. STATE HOMELAND SECURITY

In reviewing state homeland security websites with information posted, all had a common theme that ventured more towards natural disaster than terrorism and few actually referred to HSAS. Not all states had information posted as to how to respond, and more importantly, each state took an individual approach to the guidance published for the public. The majority of the states have taken an all hazard approach and combined natural disasters with terrorist attacks into common preparedness and response plans, for which HSAS was not designed.

As mentioned, the states varied in their approach and a sampling was selected for this review primarily based on the states the author was most familiar with as part of his work in coordinating terrorist related exercises. States outside this region were also reviewed to provide a contrast, particularly after seeing the trend of little if any guidance being published as to what the different threat levels meant and how the public should respond.

Pennsylvania has a very straightforward and simple approach and basically copies the Homeland Security site describing HSAS without providing additional information to the public (Commonwealth of Pennsylvania Office of Homeland Security, 2002). South Dakota, on the other hand, does not mention HSAS on its homeland security website other than the current national level, but with no mention of the aviation sector. The South Dakota site describes the mission of homeland security and offers information and links to other sites, but does not prescribe any specific guidelines for implementing changes to HSAS (South Dakota Office of Homeland Security, 2008).

Wyoming has even less information and refers the public to www.ready.gov while outlining some basic steps to take during any type of emergency. Reference to HSAS is not made on the site including the current threat level (Wyoming Office of Homeland Security, 2008). Utah is very similar in that it is focused more on natural disasters than a terrorist threat and again no reference to the current threat level is made (Utah Department of Public Safety, 2008). Nebraska also does not display or reference HSAS, but does provide links to the DHS and Red Cross sites to obtain information (Nebraska Emergency Management Agency, 2008).

The North Dakota Division of Homeland Security works with North Dakota communities with a common goal of protecting citizens, critical infrastructures, and the assets they control. In the wake of 9/11, each North Dakota community adopted heightened security measures with private, public, and individual partnerships emphasizing the necessity to report any suspicious activities in neighborhoods, schools, workplaces, high-profile, heavily-attended events, and key facilities. North Dakota has evaluated and adjusted training and operational initiatives, incorporated aviation security measures, heightened security of key facilities, increased intelligence gathering and sharing among law enforcement, military, and public agencies, enhanced direct communications with federal counterparts, and launched public information campaigns designed to empower individuals and organizations at the local level. Along with these activities, the North Dakota Terrorism Protective Measures Resource Guides provide an overview of terrorist threats facing key assets within the state and measures to protect them. The guides are intended to give information and assist in determining areas within

these critical facilities vulnerable to possible terrorist attacks and ways in which to protect them. Despite all the measures taken by North Dakota, HSAS or current threat levels are not mentioned or displayed (North Dakota Department of Emergency Services, 2008).

The Colorado Division of Emergency Management (CDEM) also has no direct guidance for HSAS, nor is the current threat level displayed on the site; however, it does discuss terrorism. The focus of its homeland security page is to downplay the terrorist threat by emphasizing that it is natural to be afraid of terrorists and their acts, and that it is also this fear upon which terrorists feed to achieve their political and social goals. It continues by highlighting that terrorism causes fear because it is difficult to predict when or where a terrorist may strike. After listing factors known about terrorists, CDEM stresses it is committed to planning for, training, and exercising emergency first responders and support agencies at the state and local level to reduce the risks of terrorism. However, preparedness is everyone's job and then lists some basic actions individuals can take for any type of disaster or emergency (Colorado Division of Emergency Management, 2008).

Iowa's Homeland Security and Emergency Management (HSEMD) website displays the current threat levels, but refers people to the DHS site for additional information. HSEMD's underlying priority is ensuring Iowa is prepared and ready to respond to any emergency or disaster. The site discusses how Iowa is more secure and better prepared to prevent, respond to, and recover from emergencies and disasters, natural or human-made as a result of a partnership between citizens, volunteer and faith-based organizations, the private sector, and state, local and federal governments. Iowa's homeland security responsibilities date back to the State Civil Defense Agency in 1965. Following 9/11, they were integrated into the duties and responsibilities of the Emergency Management Division (EMD). The EMD assumed the responsibilities for developing and coordinating the implementation of a comprehensive state strategy to secure Iowa from terrorist threats or attacks and was renamed in 2003 to reflect the homeland security and emergency management missions. Since Iowa is more likely to

face floods, tornadoes, and hazardous materials spills than a terrorist attack, many of the steps taken to prepare for emergencies apply to both terrorism and other disasters (Iowa Homeland Security and Emergency Management, 2008).

In contrast to the above-mentioned states, California takes a different approach, and after describing HSAS, lays out the specific measures to be taken under each threat level. The measures are additive and increase as the threat level rises with a total of 95 measures that could be implemented. These measures are only recommended and not required to be implemented. Each department or agency within the state is responsible for determining which actions and plans are appropriate to implement for their organization (Governor's Office of Emergency Services, 2003).

Alaska is also pretty much in line with California in that the current levels are displayed and specific measures are listed for each threat level. These measures are currently in draft and are broken down by threat level and matrixed against critical facilities protective actions, state and local government actions, and anticipated public response. As with California, these measures are additive as the threat level increases (Alaska Division of Homeland Security and Emergency Management, 2008).

The Alaska Department of Military and Veteran Affairs webpage displayed the HSAS threat levels in comparison to the DoD FPCON levels. The site indicates that the two systems were not developed to be a mirror image of each other. Instead, the Homeland Security System was developed to be an advisory system and complements the DoD FPCON system. Figures 5 and 6 display a comparative view of the HSAS versus the FPCON with a description of each. This comparison shows how closely they are related (Alaska Department of Military and Veteran Affairs, 2002).

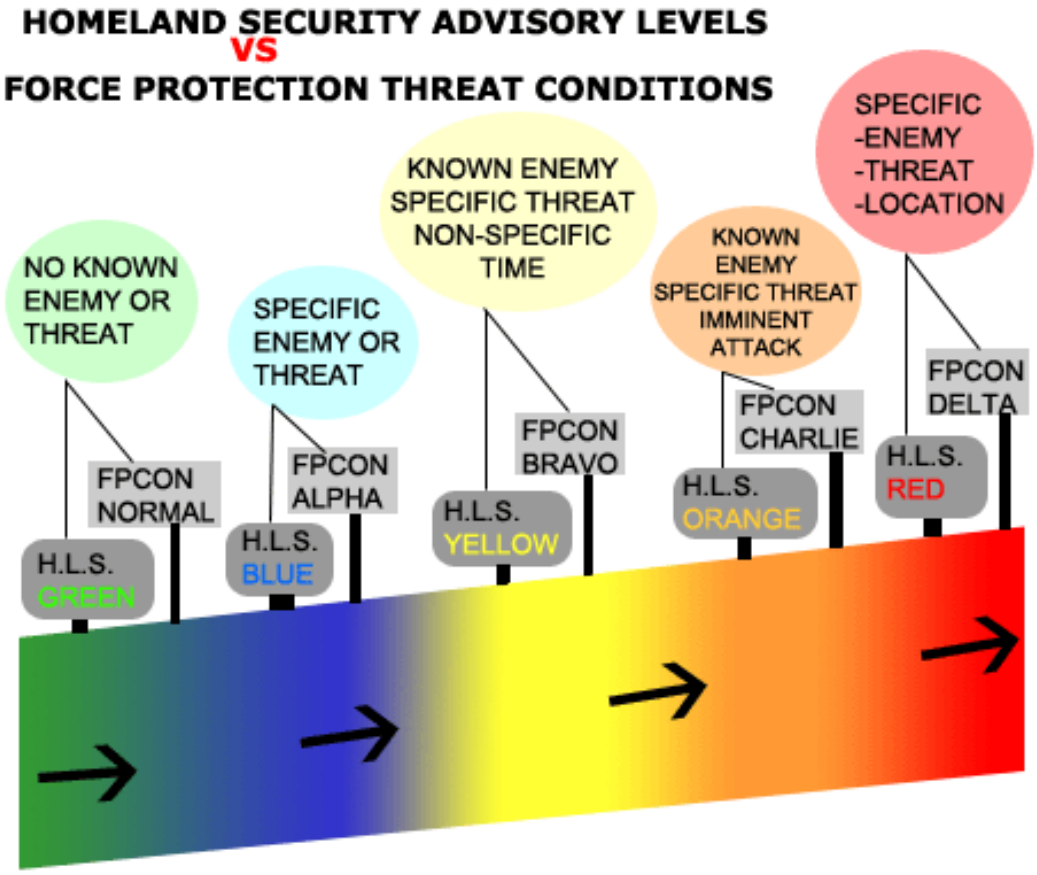

Figure 5. HSAS vs. FPCON Levels (Diagram) (From: Alaska Department of Military and Veteran Affairs, 2002)

GREEN—Low	FPCON NORMAL
• Be aware of surroundings • Know how to turn off power, gas, & water • Know where HAZMAT is stored & proper disposal methods for unneeded chemicals • Know back-up systems (generators, flashlights, etc.) • Note routines & exceptions to routines	• Applies when there is no discernible terrorist activity • Under these conditions, only a routine security posture, designed to defeat the routine criminal threat, is warranted. • The minimum FPCON for U.S. Army commands is NORMAL.
Blue—Guarded	**FPCON ALPHA**
• Key leaders become familiar with emergency response & business resumption plans • Develop a communications plan for emergency response & key personnel. • Review, update & practice plans for higher levels • Review security for access control to sites	• Applies when there is a general threat of possible threat activity against personnel and/or installations • The nature and extent of which is unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures • Commands must be capable of maintaining FPCON ALPHA measures for extended periods, with only limited impact on normal operations
Yellow—Elevated	**FPCON BRAVO**
• Continue lower threat conditions procedures • Announce ELEVATED condition to employees • Notice & report non-routine / suspicious activities • Identify & monitor information-sharing sources • Update & test emergency response & key personnel contact lists • Coordinate emergency plans by jurisdiction • Review & practice employee security procedures	• Applies when an increased or more predictable threat exists • Commanders must be able to maintain measures for several weeks without substantially affecting operational capabilities, or aggravating relations with local authorities and members of the local civilian or host nation community.

Orange—High	FPCON CHARLIE
• Continue lower threat conditions procedures • Announce HIGH conditions to employees & explain anticipated actions • Monitor world & local events • Ensure security measures are all in place • Report all suspicious activities & objects • Search all personnel and items • Restrict "close-by" vehicle parking	• Applies when an incident occurs or intelligence is received indicating imminent terrorist action • Implementation of FPCON CHARLIE measures for more than a short period will probably create hardships for personnel and affect the peacetime activities of units and personnel
RED—Severe	**FPCON DELTA**
• Continue lower threat conditions procedures • Announce SEVERE condition to employees • Immediately report suspicious activity to law enforcement • Deploy security personnel based on threat • Restrict entry & parking access at critical sites • Maintain close contact with law enforcement • Provide security in parking lots & company areas • Restrict/suspend all deliveries to critical sites	• Applies when a terrorist attack has occurred, or intelligence indicates likely terrorist action against a specific location • Normally declared as a localized warning and requires implementation of mandatory security measures • Commanders are authorized and encouraged to supplement these measures. • Implementation of FPCON DELTA cannot be sustained by commands for extended periods without causing significant hardships for personnel and affect the peacetime activities of units and personnel

Figure 6. HSAS vs FPCON Levels (From: Alaska Department of Military and Veteran Affairs, 2002)

D. DEPARTMENT OF DEFENSE

DoD installations are exempt from following HSAS as it operates under its own threat advisory system known as Force Protection Conditions (FPCON). This system has five levels: Normal, Alpha, Bravo, Charlie, and Delta, which represent increasing levels of terrorist threat. Along with each level are mandatory minimum protective measures implemented at each unit within an installation. The FPCON is based on a variety of information including threat and vulnerability assessments from various sources.

Individual installation commanders can also implement additional measures based on their local assessment providing flexibility within the system. The HSAS and FPCON systems are not tied to each other, but are based on the same intelligence (General Accounting Office, 2004b, pp. 42–43).

DoD Instruction 2000.16 dated October 2, 2006 paragraph E3.22 is the guidance and standard for FPCON measures. This instruction gives geographic commanders anti-terrorism authority and responsibility for all DoD personnel, including family members, to include establishing a baseline FPCON and to ensure that measures are uniformly disseminated and implemented. One of the key components of this instruction, paragraph E3.22.2.2, establishes a review mechanism to lower FPCON levels as soon as the threat environment permits. This mechanism is essential as remaining at elevated levels for an extended duration is counterproductive to effective security. Enclosure 4 from DoDI 2000.16 specifically discusses FPCON measures and how they progressively increase protective measures in anticipation of or in response to a terrorist attack. The measures assist commanders in reducing the risk of terrorist attack to DoD personnel. Enclosure 4 provides a definition for each of the five levels along with detailing measures for implementation at each level (Department of Defense Instruction (DoDI) 2000.16, 2006).

Joint Publication 3-07.2 Appendix J further outlines the terminology and definitions of the FPCON measures to ease inter-service coordination and support antiterrorism activities. It states the purpose of the FPCON system is accessibility to and dissemination of appropriate information. The declaration, reduction, or cancellation of specific FPCON levels belong to the appropriate commander based on this intelligence (Joint Publication (JP) 3-07.2, 1998). As a geographic commander, the Commander of U.S. Northern Command (USNORTHCOM) determines the minimum force protection level for installations located within the continental United States and is responsible for defending the homeland and providing defense support of civil authorities. While USNORTHCOM establishes the minimum level, individual installations can raise the level based on their risk assessments. Currently, the majority of military installations are at Alpha, which indicates a general threat of possible terrorist activity (USNORTHCOM News, 2007). This level would equate closer to guarded (blue) on HSAS rather than

elevated (Yellow) that indicates a significant risk and at which this nation has been for over six years.

FPCON levels as described in Air Force Manual 10-100 are progressive levels of terrorist threats and initiate pre-planned actions. FPCON declarations are normally provided through the chain-of-command, public address systems, or other available resources (Air Force Manual 10-100, 2004, p. 19).

Condition	Application	Considerations
FPCON NORMAL	Applies when a general global threat of possible terrorist activity exists.	Warrants a routine security posture.
FPCON ALPHA	Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature, and extent of which are unpredictable.	ALPHA measures must be capable of being maintained indefinitely.
FPCON BRAVO	Applies when an increased or more predictable threat of terrorist activity exists.	Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.
FPCON CHARLIE	Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.	Implementation of CHARLIE measures will create hardship and affect the activities of the unit and its personnel.
FPCON DELTA	Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent.	Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

Figure 7. Force Protection Levels (From: Air Force Manual 10-100, 2004, p. 19)

III. HSAS CRITIQUES

From its very inception, HSAS suffered from attacks on its credibility. Comedians began joking about the color-coded levels and various mock systems began popping up on the internet. Charges that HSAS was being used for political purposes began to surface and news outlets stopped running banners across TV screens with the current threat level. As years passed, the critiques became harsher as no credible information was provided to back up raising the threat levels and no closure was provided when they were subsequently lowered. While protective measures provided guidelines for law enforcement officials to follow, they did not provide instructions for the general public. According to a poll conducted by the Anser Institute for Homeland Security (data retrieved on April 19, 2002), 31 percent of the respondents said HSAS will be somewhat or very effective in informing the public of potential terrorist attacks, while 43 percent say it will be somewhat or very ineffective. HSAS was already drawing negative reviews only a month after the announcement (Center for Defense Information Terrorism Project, 2002).

A. SYSTEM CRITICS

The advisory system was not without critics. Arguments have ensued that the administration has not fully defined the threshold for a change to the threat level.

> Ridge's warning lights are meant to reflect the terrorist threat, but instead they are cause for confusion and a staple joke on late-night television, writer John Miller said in a June 2002 edition of The National Review. People don't need a set of lights with vague significance; they need useful information and practical advice. (Online NewsHour, 2003)

Following a Federal Bureau of Investigation (FBI) warning to police about a possible "spectacular" al-Qaida attack planned against the United States and its interests, a warning that did not spark a threat level boost, *The New York Times* asked how Americans could be asked to prepare against a terrorist strike without more precise information:

> The only thing warnings this vague are good for is providing political cover in case of disaster, the Times wrote in a Nov. 17 editorial. They offer no specific information about the location, timing or method of attack, and are all but useless to the average citizen, or even to local law enforcement officers. (Online NewsHour, 2003)

Other critics said it is more appropriate for specific warnings to come from local or state governments rather than the federal advisory system.

> Nobody knows what the color levels mean. That's okay, they're declaring a level for the entire country. But the further down you drill, the more specific you need to become. Washington, D.C. Deputy Mayor for Public Safety Margret Nedelkoff Kellems told The Washington Post in November. (Online NewsHour, 2003)

Despite the criticism and jokes about how the system was designed, Secretary Ridge stated state and local law enforcement officials are pleased with the system because it allows agencies to work from the same page.

> [The advisory system] was embraced by the 50-plus homeland security advisers because we all think we need a standard vocabulary that says to the country what level of risk we're at, Ridge said in May. I think the system is working very well. (Online NewsHour, 2003)

As established under HSPD-3, HSAS was designed for the federal government and left states, communities, and industry to establish their own responses (Bush, 2002). In response, non-governmental agencies, states, and industrial sectors have worked to fill this void. Although well intended, this approach has no standardization and still leaves the public uninformed without a strong informational process to disseminate the information.

Across the country, questions of "what does a condition 'yellow' mean to me or my family?" or "What does this mean to a business or school?" remained. The American Red Cross recognized the need and developed a complementary set of guidelines for the following areas: individuals, families, neighborhoods, schools, and businesses. Each of these guidelines is based on HSAS, provides actions to be executed, and is available on the Red Cross website (American Red Cross, 2003).

One of the most extensive and critical articles on HSAS was written by Jacob Shapiro and Dara Cohen in 2007 entitled Color Blind: Lessons from the Failed Homeland Security Advisory System and published in the *International Security Journal*. They specifically ask if the system works, and if not, what are the central problems and how might they be mitigated or eliminated. Their primary argument is that the system is based on the confidence of those making the decisions, but that over time, HSAS came to be seen as politically manipulated, and ultimately, has failed. With no statutory authority to order specific measures from state and local governments or private industry, the system has to fall back on the confidence generated from the information and that the costs of protection are less than the expected losses. HSAS has not met that level and the result can be seen by the lack of response by state and local governments and confusion amongst the general public. In their view, the problems with the current system have not been addressed in any existing critiques, and ultimately, propose an alternative system that in their opinion solves the major flaws in the current system. Their alternative system would correct the main flaw in motivating protective actions by requiring the federal government to pre-negotiate a set of measures with industry and governments for each advisory level. They argue specificity about the threat would be ensured and the actions to reestablish trust and confidence in the system would be taken (Shapiro & Cohen, 2007, pp. 121–123).

The first section of their article covers the origin and gradual failure of HSAS, which having already been discussed in this thesis, is not repeated in this section. After describing the origins, Shapiro and Cohen discuss the political manipulation of the system dating back to February 2003 just prior to the Iraq war. They document a 2003 poll that indicated only 9 percent of individuals made any changes to their daily routines. They contend that decreasing trust along with a lack of federal funding have led to a steady decline in responsiveness. In response, DHS created regional alerts versus the broad national alerts and set internal guidelines that would raise the alert level based only on credible intelligence. Despite these adjustments, by the time of the 2004 presidential election, 40 percent of the population believed that increases in the alert level were politically motivated. This increasing distrust of the system led to state and local

governments dropping HSAS from their planning. The random nature of when levels were increased or lowered without specific threats sent a message that the system is arbitrary and not linked to actual threats. Per the authors, by the beginning of 2006, HSAS had failed as a system yet they emphasize it has served a valuable service in providing a common language between states and advances in public warnings issued by states (Shapiro & Cohen, 2007, pp. 123–132).

In their discussion of other international alert systems, Shapiro and Cohen begin by stressing that most differ significantly from HSAS. Again, with a review of other systems already provided, a full review is not given in this section. The additional country they mention is Israel and how the government issues alerts to the military and law enforcement agencies, and on occasion, to the media for dissemination to the public. They highlight that Israel is more concerned with specificity to avoid overwhelming the populace with constant alerts (Shapiro & Cohen, 2007, pp. 132–135).

Shapiro and Chen then discuss the logic of terror alerts with the ultimate goal of the government being to prevent an attack, deter, divert, or defer an attack, or to mitigate the consequences of an attack. They assert that public alert systems, if trusted, may create the incentives to generate deterrence, and ultimately, restore public confidence in the system. They also underscore that some insist HSAS exists only to protect government officials from blame and to keep terrorism as a political topic. The basic logic is presented as a formula using the probability of an attack and an alert being issued that can in reality be boiled down to a basic risk equation (Shapiro & Cohen, 2007, pp. 135–141).

The authors argue that HSAS possesses three weaknesses: contradictions and tensions inherent in the system reduce its credibility, it is extremely sensitive to wrong assumptions about how agents will react due to no defined actions, and the complexity of the system can lead to unexpected secondary effects. Shapiro and Cohen underline that the first weakness is not inherent in alert systems but due to the construction of HSAS. The other two weaknesses can plague any alert system. They contend that combined these problems have significantly diminished the value of HSAS and contributed to its irrelevance. Contradictions exist in the system as it only applies to the federal government, yet state and local authorities are expected to respond, and while only

intended to trigger government actions, has been used as a public warning system. Even government agencies have reported uncertainty as to appropriate protective measures, which have resulted from a lack of specific pre-arranged actions to be taken not only at the federal level but also down to state and local levels, as well as industrial sectors. This uncertainty can lead to unexpected consequences when anticipated actions are not executed at lower levels or conflicting warnings or alert levels leave authorities unsure how to respond (Shapiro & Cohen, 2007, pp. 141–149).

In their final section, Shapiro and Cohen propose an alternative structure. After offering their argument as to why legislation alone will not fix the system, they review the problems with the current system, diminished impact on subsequent alerts, contradictions and confusion reducing trust, wrong assumptions about actions being taken, and systemic complexity. They recommend a system that maximizes trust without revealing damaging information. The first step is to develop specific actions available at each alert level and formalize the process. They suggest a system in which an alert is generated at a specific level with additional measures for a specific region. Standards would have to be established for what type of intelligence it would take to trigger an increased alert. This alternative system possesses four advantages: reduces the need for negotiations during a crisis, reduces confusion by having pre-existing measures, reduces the number of wrong assumptions being made, and reduces the systemic complexity by removing incompatibilities in plans. In resolving the current weaknesses and restarting the process at the ground level, a system could be developed that would regain the trust of the public (Shapiro & Cohen, 2007, pp. 149–154).

B. COMMUNITY AND STATE RESPONSE

In a similar vein, Roger Kemp, city manager of Vallejo, California, authored an article for the October 2005 *Public Management Journal* entitled Homeland Security: Common-Sense Measures to Safeguard Your Community. In his article, Mr. Kemp provided a checklist of items that local officials should take so that citizens know they are being protected. Since the United States has never been below threat level yellow, his suggested measures are based on raising the threat level to orange. The checklist includes

recommended items for citizens and business personnel in addition to the city government. His recommendations include placing a community's response measures into hard copy and distributing to appropriate personnel along with posting it on a community website for local citizens. His goal is to have the community prepared and using simple guidelines represents a common-sense approach (Kemp, 2005).

In an article published in the September 2007 edition of the *Journal of Contingencies and Crisis Management*, Christopher Reddick examined homeland security preparedness and planning. He analyzed data from city managers and the key result indicated a high level of collaboration between city government and other levels of government. One important aspect of his study was that in their planning, city managers did not view HSAS as being extremely effective. Thirty-two percent of the city managers responding to the survey considered HSAS to be ineffective and it was also perceived negatively (Reddick, 2007, p. 163).

Each time the alert status is raised, state and local communities spend resources to guard critical infrastructure, increase patrols, and staff emergency operation centers, which can place a significant strain on states and communities already facing budget cuts. In July 2003, The Council of State Governments conducted a teleconference to examine possible solutions to this issue and look at best practices (Homeland Security Brief, 2003).

Prior to 9/11, many state and local governments already had warning systems in place that either followed a numbering system or were similar to the DoD system. Most were established for government officials and agencies and required little communication or coordination with the private sector or the public. Another problem was the lack of standardization across jurisdictions. Following the attacks on 9/11, the need for a national system that could better communicate the threat across the full spectrum was realized, which is a standardized system with a basic vocabulary and framework for national preparedness (Homeland Security Brief, 2003).

With the implementation of HSPD-3, most states adopted HSAS that allowed conformity with other states and the federal government. However, the lack of well-defined protective measures has led each state and business sector to develop their own, with a resulting lack of uniformity (Homeland Security Brief, 2003).

The article reviews the expenses public agencies spend during increased alerts and mentions a survey by the U.S. Conference of Mayors taken in 2003 that it cost cities $70 more per week to be at orange rather than yellow due to overtime pay for initial responders, emergency operation centers, and the use of the National Guard. Representative John Milner of Illinois in particular notes two issues (Homeland Security Brief, 2003).

> First, the federal government issued blanket warnings and threats. In doing so, states have been faced with doing too little or too much and given the gravity of terrorism today, states are opting for the latter, and rightfully so.
>
> Secondly, states themselves are working through a long process of conducting vulnerability assessments and without a clear understanding of infrastructures and vulnerabilities, states are finding it difficult to develop sound strategies for each alert level.

As a result, states are struggling to define protective measures for each advisory level. Without a quantifiable output or cost-savings to measure, officials are feeling political pressure to reduce spending on protective measures. In addition, a critical challenge for state governments is working with the private sector and meshing the states' system with the industrial sectors advisory system (Homeland Security Brief, 2003).

The states face additional challenges in combating complacency during alert level changes, addressing the lack of uniformity and coordination amongst states regarding protective measures, coordinating with cities and counties, and educating and communicating with the public. The federal government is also aware of these issues and determining areas that need improvement using national level exercises. One issue the article did highlight is whether a need exists for five levels and will it ever be possible to reach the green/blue level or will yellow become the new low risk level. Despite the

challenges, flexibility is built into the system to allow states and communities to determine their protective measures and the resources they want to commit (Homeland Security Brief, 2003).

C. INDUSTRIAL SECTOR RESPONSE

In a letter to Robert Mueller, then director of the Federal Bureau of Investigation, North American Electric Reliability Council (NERC) President Michehl Gent (personal communication, April 26, 2002), provided the electricity sector comments on HSAS. The North American Electric Reliability Council's Critical Infrastructure Protection Advisory Group (CIPAG) developed these comments. The electricity sector supported the development of HSAS and asserted that it could assist in responding to the current threat environment. In combination with HSAS, the electricity sector had developed a threat alert system out of necessity subsequent to September 11, 2001. The Threat Alert Levels and Physical Response Guidelines were published November 26, 2001 (North American Electric Reliability Council (NERC), 2002a).

The NERC Critical Infrastructure Protection Working Group (CIPWG) developed the electricity sector threat alert system, which was designed to meet unique requirements of the electricity systems of both the United States and Canada. The alerts can be applied on a geographic, organizational, specific site, or type of facility. Specific actions (guidelines) are recommended for each of four defined threat levels that were designed specifically for the electricity sector after a thorough evaluation of alternatives. CIPAG encouraged DHS to establish a similar well-defined four-level system. In addition, it encouraged DHS to include natural disasters in regional advisory levels (North American Electric Reliability Council (NERC), 2002a).

The original version of the electricity sector alerts as published in 2001 listed five goals (North American Electric Reliability Council (NERC), 2002a).

- Define threat alert levels
- Provide guideline examples of security measures to be considered
- Ensure the electricity alert levels are consistent with threat information

- Ensure threat information is included in the threat alerts
- Issue the alerts for a specific region, city, or type of facility

The threat levels in the initial version were established as normal, low, medium, and high. Each of the levels had associated response guidelines for the electrical sector to consider. The response measures were not all inclusive and additional measures could be added (North American Electric Reliability Council (NERC), 2002a). CIPAG updated the alert system on October 8, 2002 with Version 2. The goals remained the same; however, the alert definitions were revised to align with the HSAS five-tiered color-coded system (North American Electric Reliability Council (NERC), 2002b).

Version 3 of the security guidelines was released on November 1, 2005. The first notable difference was that the goals were reduced to the following (North American Electric Reliability Council (NERC), 2005).

- Provide examples of security measures to be considered
- Achieve uniformity in response actions across the electricity sector

However, the major changes in Version 3 were the addition of a process for communicating changes in the threat level alerts by combining the threat levels with the response measures, and increasing the number of measures to be considered (North American Electric Reliability Council (NERC), 2005).

While federal agencies are required to implement specific measures to reduce vulnerabilities, state and local governments are only recommended to take similar actions. Meanwhile, the private business sector has been left on its own accord. As seen above, the electricity sector has established guidelines; however, over half of American businesses are not ready for security-related threats (Schmidt, 2004). A survey conducted by the American Management Association in 2003 indicated 64 percent of businesses have basic crisis management plans, 45 percent have specific plans, and only 42 percent conducted drills or tested their plans (Schmidt, 2004).

A primary reason for this lack of preparedness is associated with the cost of increasing alert levels. However, unlike the government, businesses can actually reduce costs by implementing comprehensive plans. A key to preventing security threats is to customize HSAS to the individual business by performing a risk assessment to evaluate

vulnerability, potential consequences, and mitigation opportunities. Schmidt indicates that many trade associations have developed industry specific measures and crisis management planning, such as the NERC. He also includes charts that suggest protective measures to be considered with each of the threat levels. He concludes that the HSAS has not erased vulnerability, but has provided a framework from which businesses can prepare for terrorism (Schmidt, 2004).

In that same regard, ASIS International has developed Threat Advisory System Response (TSAR) Guideline. The initial document was published in 2004 with a second edition released in 2008, and is applicable and designed for the private sector to assist in providing the appropriate level of security and reduce the risk of a terrorist event. The Guideline emphasizes that with 85 percent of the national infrastructure under the control of private business and industry, they will play a significant role in mitigating the effects and costs of an incident and that the public-private partnership is a crucial component of the national strategy for combating terrorism (Asis International, 2008).

The Guideline provides private business and industry a tool for consideration of possible actions that can be implemented based upon the HSAS alert level. The Guideline is a baseline from which protective measures can be enacted and does not anticipate all incidents nor does it provide specific recommendations, but can be tailored by any organization to fit its needs. The first measure recommended by the Guideline is for users to conduct a risk assessment of their facilities, infrastructure, and personnel. Ideally, this assessment would be done at a low level of threat before the condition is elevated. The measures recommended are cumulative and build upon each other as the threat increases; therefore, measures already in place should remain in effect (Asis International, 2008).

It is notable that ASIS has combined the green and blue levels into one combination and consider that many of the recommended measures at this level have already become routine. As a result, the Guideline is broken into four levels with measures recommended for emergency response–business continuity, personnel protection, and physical protection. The actual matrices are easy to read and use, and provide a baseline response for any organization/industry that can be utilized for natural disasters, as well as terrorist incidents (Asis International, 2008).

IV. HSAS FLAWS

The General Accounting Office (GAO) and the Congressional Research Service (CRS) independently conducted studies of HSAS and determined flaws that needed to be addressed.

A. GENERAL ACCOUNTING OFFICE

The GAO issued a report on February 26, 2004 covering information obtained from a questionnaire sent to federal agencies along with information gathered from states and local governments based on their critical infrastructure. This report reviewed five specific areas of concern (General Accounting Office, 2004a).

- The Advisory System includes threat analysis, notifications, and ongoing revisions, but protocols for notification have not been documented
- Federal, state, and local agencies reported receiving useful information and guidance, but would prefer more specific information
- Federal agencies reported enhancing existing protective measures more often than implementing new measures, while state and local agencies reported implementing additional measures
- Cost data reported by federal, state, and local government agencies is limited
- Some federal, state, and local government agencies have similar advisory systems, but can change threat levels independently

A second report issued by GAO in June 2004 covered some of the same aspects of the previous report but examined the following specific areas (General Accounting Office, 2004b).

1. The Decision-Making Process for Changing the National Threat Level

The national threat level is assigned by the Secretary of Homeland Security, in consultation with members of the Homeland Security Council, based on analysis of intelligence information and assessment of the vulnerability of potential terrorist targets. This same assessment is used to determine whether specific industrial sectors or geographic regions should operate at heightened levels (General Accounting Office, 2004b, p. 4).

2. Guidance and Other Information Provided to Federal Agencies, States, and Localities, Including the Applicability of Risk Communication Principles to Information Sharing

No documented protocol exists for providing threat information to federal agencies and states. The reason given by DHS officials is that it has been difficult to develop a protocol that provides flexibility for sharing information in a variety of situations. Risk communications experts suggest that to ensure comprehensive information dissemination, threat warnings should consist of the following: communication through multiple methods, timely notification, and specific threat information and guidance on actions to take. While DHS uses multiple methods to communicate threat information, many federal agencies and states responded that they first learned about changes from media sources rather than official channels. They also reported that they did not receive specific threat information or guidance, which hindered their ability to implement protective measures (General Accounting Office, 2004b, pp. 4–5).

3. Protective Measures Federal Agencies, States, and Localities Implemented During High-Code Orange-Alert Periods

Some federal agencies reported that they regularly operate at high levels of security, and therefore, did not have to implement a substantial number of additional measures to respond to code-orange alerts. In contrast, states indicated that factors, such as specific threat information, influenced the extent to which they implemented additional measures. Both federal agencies and states indicated that increased protective measures adversely affected their operations. A specific comment was that multiple government agencies providing conflicting information limited the states' ability to coordinate and implement measures (General Accounting Office, 2004b, p. 5).

4. Additional Costs Federal Agencies Reported for Implementing Such Measures

Cost data reported by federal agencies did not include all additional costs and may not have been reliable. However, despite these limitations, the data was sufficient to be an indicator of general trends. Some federal agencies reported no additional costs as they

had already implemented protective measures or redirected existing resources; however, they may not have accounted for indirect costs (General Accounting Office, 2004b, p. 6).

5. Information DHS Collected on Costs States and Localities Reported for Periods of Code-Orange Alert

Information collected from various state and local sources on the costs associated with elevating the threat level did not represent all additional costs incurred. As a result, the reported information may not be adequate for making generalizations regarding incurred costs during periods of heightened response for federal, state, and local agencies (General Accounting Office, 2004b, p. 7).

B. CONGRESSIONAL RESEARCH SERVICE

CRS was asked to review HSAS, and issued an initial report on August 6, 2003 with several subsequent updates. The CRS report concluded that while the need for terrorist threat warnings seems to be widely acknowledged, numerous issues were associated with HSAS and its effects on states, localities, the public, and the private sector. Issues with HSAS as noted by CRS include the following (Reese, 2003).

1. Vagueness of Warnings

With each change in threat condition, intelligence information was cited but offered little specificity, such as region, state, or city. Moreover, DHS has never explained the sources and quality of intelligence upon which the threat levels were based (Reese, 2003, p. 4). The assertion is that when federal government officials announce a new warning about terrorist attacks, the threats are too vague and that the public may begin to question the authenticity of the HSAS threat level. The concern is that if the credibility of the system is questioned, the public may wonder how to act or whether to take any special action at all, which could eventually lead to complacency (Reese, 2003, p. 5).

2. Lack of Specific Protective Measures for State and Local Governments, the Public, and the Private Sector

HSAS provides protective measures for each threat condition, but are identified only for federal agencies. DHS only recommends protective measures for states, localities, the public, or the private sector; however, the recommended protective measures are the same ones issued to federal agencies. HSAS silence with regard to protective measures for the public, the private sector, and state and local governments has drawn the attention of some interested observers. Citing what some contend is a lack of DHS guidance on protective measures; non-federal entities are beginning to fill the perceived void (Reese, 2003, p. 6).

3. Communication of Terrorist Threats to State and Local Governments, the Public, and the Private Sector

DHS uses a variety of communications systems to provide terrorist threat warnings to states, localities, the public, and the private sector, including state and major urban area fusion centers; also at classified levels. The public is alerted to a change in a HSAS threat condition through the news media, following a public announcement from DHS or media leak of the information. No Emergency Alert System type communication is activated to alert the public to a change in threat condition. Therefore, the public is not informed of the change until they monitor a public news source (Reese, 2003, p. 8).

4. Coordination of HSAS with Other Warning Systems

HSAS is not the only federal warning system to provide timely notification about imminent and potentially catastrophic threats to health and safety. Some argue for the consolidation of the existing warning systems into one "all-hazard" system. Consolidation and coordination of these warning systems would present challenges to administering an "all-hazard" warning system. Some of the challenges include the administration of the warning system, interoperability of existing warning systems, and the involvement of industry. Consolidating and coordinating federal warning systems, however, may cause a loss of concentration on the systems' traditional hazards. Mature

warning systems have established alerting protocols and routines that, if consolidated, could become too broad, which may result in less effective warnings (Reese, 2003, pp. 9–11).

5. Cost of Threat Level Changes

An increase in the HSAS threat level imposes both direct and indirect costs on federal, state, and local governments, the private sector, and the public. These costs include the increased security measures undertaken by states and localities, loss to tourism, and the indirect cost on the economy during a period of heightened threat level.

Local governments incur direct costs when they put in place additional security measures to deal with a higher threat condition. Due to the budget crisis that many states are experiencing, additional homeland security costs during heightened threat periods are seen as an additional fiscal burden. An indirect cost of a heightened threat level is the negative effect on tourism in cities perceived as potential targets of terrorism. Some municipal officials have had to make a costly decision between homeland security and tourism (Reese, 2003, pp. 12–13).

Authorized program expenditures are another point of contention that states and localities have with homeland security funding and costs. All homeland security grant programs list authorized equipment and activities that grant allocations can be used to fund. States and localities may argue that these authorized expenditures do not address their specific homeland security needs (Reese, 2003, p. 13).

These direct homeland security costs occur not only at the state and local level when the threat level changes. Federal departments and agencies have to adopt prescribed protective measures outlined in the different threat condition levels of HSAS (Reese, 2003, p. 13).

In addition to discussing the flaws in the system, the most recent report discussed Congressional actions that have been proposed. The first would have required DHS to establish a telephone alert network to warn the public of terrorist incidents and disasters and would provide information on protective measures. Another proposed establishing a

National Alert Office within the National Oceanic and Atmospheric Administration. The final proposal would have required DHS to change the current system to require information on the threat and protective measures be included in the warnings. The warnings would also have been limited to a specific region, locality, or economic sector, and would have required issuing warnings without the use of the color designations (Reese, 2008).

V. PSYCHOLOGY OF TERRORIST WARNINGS

While cities and government agencies faced a financial burden instituting threat level changes, individuals faced an entirely different aspect. The fear of living under continued levels of high risk of a terrorist attack placed a psychological burden on individuals who were not being provided with all the details regarding a threat. Initial responders were becoming worn down both physically and psychologically from working overtime. Even without conducting attacks, terrorists were gaining the upper hand and attaining their goals. The Center for Defense Information Terrorism Project stressed that HSAS was created in part to a response to criticism received each time the Homeland Security Office announced public warnings of terror attacks after 9/11. Four warnings were issued from October 2001 and February 2002 before HSAS came into existence. No terrorist attacks followed the warnings so it is not obvious whether the warnings helped prevent attacks or eroded the credibility of the warnings. Government officials and the public complained that the warnings urged citizens to be prepared for an attack without providing any specifications of time, location or type. Many questioned the utility of the warnings, and believed they merely propagated public fear (Center for Defense Information Terrorism Project, 2002).

Rose McDermott and Philip Zimbardo in an article entitled "The Psychological Consequences of Terrorist Alerts" state that in reality only two real colors exist despite having been created with five colors. The rationale is that red actually means the nation is under attack and no politician is willing to lower the level below yellow for fear of an actual attack occurring. The authors emphasize that terror alerts produce both political and psychological effects. Politically, first responders and the public increase their vigilance. However, terror alerts can also result in negative outcomes, such as negative public mental health outcomes (without a commensurate increase in security), increased depression, and posttraumatic stress disorder. In addition, these alerts encourage unthinking support for charismatic leadership; and pose a threat to diverse political culture. Their main argument is that the current system does the terrorist's work for them

by inducing anxiety, depression, and paralysis in the population, and through their discussion, offer suggestions for a more effective and less destructive system (McDermott & Zimbardo, 2007, pp. 358–359).

The authors highlight that during the first six terrorist alerts issued following 9/11 alleged to have reliable information from "credible" yet unnamed sources warning of an imminent attack somewhere, sometime soon, in the United States or elsewhere in the world, against it offices or agencies. The very vagueness of these warnings following on the heels of 9/11 created high levels of fear and anxiety for ordinary citizens. With no concrete actions to take other than being vigilant, citizens were further confused when told to "go about your business as usual." McDermott and Zimbardo ask how it is possible to "go about your normal business" after being told of an increased threat of a terrorist attack, which ultimately leads to a feeling of helplessness. This situation was worsened when no additional attacks occurred, but the government also did not offer any explanation when the threat level was decreased. Where had the terrorist threat gone? After following this process during multiple alerts, the authors assert that habituation effects set in, and people cease to respond to the danger or take appropriate actions without knowing the results of previous actions taken. In effect, citizens became desensitized to the high alert level and found themselves trapped in the conundrum of being inured to report suspicious events or individuals, but too anxious to return to normal life (McDermott & Zimbardo, 2007, pp. 359–360).

With the advent of the color-coded alert system, one voice indicating that the information came from multiple intelligence sources, a list of potential "soft" targets, and worst case scenario thinking as to the weapons the terrorists were likely to use, it appeared that the warning process had improved. Even a shopping list of actions citizens could take to be prepared was created. Experts provided information on security measures and warnings were placed on the DHS website. At the same time, the Orange alert level was announced and individuals were seen taking the prescribed actions. However, when no attack occurred again with any explanation from the government, and then learning that some of the intelligence may have been a hoax, credibility of the system suffered (McDermott & Zimbardo, 2007, pp. 360–361).

With the installation of fear and anxiety into civilians being accomplished by the government through mismanaged terrorist alerts and the spending of limited resources in anticipation of attacks that never occur, the terrorists' work is being done for them. The authors throw out the possibility that the terrorists having seen the frenzy caused by the alarms and having learned lessons from the past, may be intentionally disseminating misinformation to keep this nation on a high level of alert, which will eventually have both an economic impact in the constant spending on homeland security, as well as a psychological impact with heightened anxiety and confusion, particularly when considering an attack has not occurred since 9/11. The authors allude that the alerts create a climate of hostility and danger that encourages political disengagement that results in more willingness to accept restrictions on personal freedoms to prevent terrorist activity. They then delve into studies that show the continued psychological toll of the 9/11 attacks and how the effects may be exacerbated or prolonged with the continued heightened levels of alert maintained under HSAS (McDermott & Zimbardo, 2007, pp. 361–363).

The authors then draw upon two theories to help explain the possible impacts of the terror alert system. Under the social identity theory, the threat of terrorist attacks would increase group identification with consequent support for leadership along with hatred of foreign groups perceived to be responsible, which is enhanced by the terror management theory that reminds people of their own mortality that results in an increased need for safety and psychological security. This theory also demonstrates that people will be drawn to those who express a similar worldview while excluding those with different views (McDermott & Zimbardo, 2007, pp. 363–364).

McDermott and Zimbardo question why the government would create and maintain an ineffective and psychologically damaging system. Their explanation is that although the system is neither ideal nor as effective as it could be, it does serve legitimate subsidiary political goals. They stress that while inefficient, the current system does provide first responders with additional funding for new equipment and training. It also provides a cover for elected officials in the event of another attack. An alternative hypothesis proposed is that leaders may manipulate public opinion using fear to gain

political power or advantage. Fear will motivate people to become more vigilant; however, high levels of fear can also prove distracting so a line must be drawn to maintain a balance. An attack can also generate anger, as was witnessed in the days following 9/11, and will make the population more supportive of government actions in conducting punitive actions, particularly as long as these actions are seen as producing positive results (McDermott & Zimbardo, 2007, pp. 364–365).

The authors suggest two limitations to the current system. First, warnings should be issued by a credible source based on specific information. People should be told the where and when of threats, and after a period of time, should also be told whether an attack was preempted or if the information was flawed. However, political implications exist in performing this act of notification. State and local governments may have the desire to disseminate the information before the federal government; in addition, it can be argued that disseminating information on certain targets may just drive terrorists to hit softer targets. A credibility issue is also involved if an alert is issued, resources spent, and no attack occurs. The second limitation is that alerts need to be tied to actual behaviors. A heightened alert level should mean more than increased vigilance or the result would be nothing more than increased anxiety and depression. Specific and realistic actions for people to take to reduce the risk and protect themselves will have positive impact. Naming specific groups or ethnicities can produce negative impacts and should be well thought out before being issued as part of an alert. Alerts should also be geographic in scope to reduce the number of individuals in the potential "worry" zone. Alerting the general public is also not always required, and in some cases, only first responders should receive the warnings. Alerting the general public in these instances may only serve to increase stress without providing any additional security. The authors propose a reexamination of how to best construct and utilize terror alarm systems and how to explain negative results to the public. Repeated false alarms could eventually lead to complacency and a lack of preparedness to respond during an actual event. High levels of sustained stress can have a destructive impact on the nation that could be worse than any actual terrorist attack (McDermott & Zimbardo, 2007, pp. 365–367).

The authors conclude with a two-track policy towards threats. First, terrorist threats should not be used for domestic political purposes as doing so reduces effective responses from the population and accomplishes the terrorists' job by placing fear into their intended targets without exposure on their part. Second, warnings should be credible, specific, timely, and designed to motivate people to take protective measures. When threats do not materialize, open dialogue should occur as to how the threat was averted. By incorporating these two measures into a reconstructed system, credibility can be maintained with more effectiveness, at less cost, and with less anxiety (McDermott & Zimbardo, 2007, p. 368).

The psychological impact of repeated changes or lengthy periods of elevated alerts need to be factored in, regardless of the threat advisory system in place. Passing on credible information and keeping the public informed are essential in an effective advisory system. The general public has enough built in fear of terrorist activity and does not need to have that increased by false warnings or elevated threat levels far beyond what may actually be required. A significant portion of this process is letting the public know that a threat has been eliminated, not just that the threat level has been reduced. While fear can be used for positive purposes, it can become difficult to have people continue their normal routines if they are suspecting everyone is a terrorist or every package contains a bomb. Terrorist alerts and raising the threat levels should be accomplished judiciously, based on credible information, established for a specific timeframe, and not be politically motivated. Using specific alerts targeting geographic areas or industrial regions will also help to limit undue anxiety in regions not being targeted.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. A COMPARISON OF TWO CITIES

The cities of San Antonio, Texas and Agency, Iowa are 1,000 miles apart, in separate regions of the country, entirely different in size and ethnic composition, but have at least two items in common. The first is that that author has lived in both, Agency for 18 years and San Antonio for eight years. The second is that both came under the auspices of HSAS.

Using two cities with such extremes may seem like stacking the deck against HSAS, but in reality, shows that the nature of the one size fits all approach did not in this event work effectively for all. It was effective as an initial product to give the country something to focus on and use to develop plans and allocate resources, but beyond those initial few months, HSAS needed an overhaul.

Under the conditions established by HSAS, both communities have been under the threat of a significant risk of terrorist attack and have had to take appropriate risk measures. Either city could be a potential target depending on the terrorists' goals; therefore, both would need to heed the recommendations provided by HSAS.

Cities like San Antonio and Agency were left to their own devices through much of the duration of HSAS. Designed for the federal government, HSAS left local communities to determine their own specific threat level responses (Bush, 2002).

A. SAN ANTONIO

Known as the home of the Alamo, and famous for its Riverwalk, San Antonio, Texas is a rapidly growing, 16 percent in the previous 10 years, multi-cultural city bisected by three Interstate highways, one of which links the two coasts while another runs from the Mexican to the Canadian border (U.S. Census Bureau, 2011). The 2010 census data lists San Antonio as the second largest city in Texas and seventh largest in the United States (U.S. Census Bureau, 2010a). With three major military installations, (Lackland AFB, Randolph AFB, and Ft. Sam Houston) and a large retired military population, San Antonio is commonly referred to as "Military City" and is annually

visited by more than 20 million tourists per year. With an economy driven largely by the tourist trade, San Antonio is also headquarters for several large corporations ranging from the energy structure to financial services and medical care.

For San Antonio, the cost of overtime for additional shifts for fire and police during periods of increased alerts would eventually put a significant dent in the city's budget, not taking into account the additional strain it would put on the limited manpower available. Then, add in lost revenues from tourists who are staying away, and the situation is compounded. Eventually, the terrorist wins by keeping San Antonio in a higher level of alert than required, which was a flaw of HSAS in that limited flexibility was provided without going against recommended advice when a threat warning was issued. The reports issued by GAO not only focused on the cost factors associated with HSAS but also the decision-making process and the manner in which the threat information was transmitted to the country (General Accounting Office, 2004a; General Accounting Office, 2004b).

San Antonio was kept under an elevated threat for years despite knowing the true nature or potential targets of the threat. As highlighted by McDermott and Zimbardo, individuals remained confused and created higher levels of fear and anxiety (McDermott & Zimbardo, 2007, pp. 359–360). In time, individuals became frustrated with the system, as no tangible evidence was presented of when an attack was prevented or where it had been aimed. The Mayor of San Antonio, just as every other large city mayor, had a vested interest to keep the threat level reduced to minimize costs and keep the flow of tourist trade and dollars.

A Homeland Security Brief from August 2003 reflected how states were struggling to define protective measures and how the costs of additional security at the higher levels were beginning to have an impact on the economy. The first chapter provides a description of the confusion caused when multiple threat levels are encountered within the confines of a city. Basically, HSAS had reached a point at which the public had become complacent about the advisory system and were doing nothing when increased levels were announced.

B. AGENCY

On the other extreme, Agency, built on the site of an Indian agency for the Sac and Fox tribe, is located in rich Iowa farmland, has a total population including rural areas of slightly more than 1,100 (U.S. Census Bureau, 2010b), is now bypassed by the nearest highway, and has no major industry other than farming.

A major factor that comes into play is the cost of implementing and maintaining the additional security measures as the threat level is increased. In a town the size of Agency with no police force and a volunteer fire department, the costs and long-range impacts are minimal. Yet, with a smaller tax base, the burden of any associated costs is greater on the individuals in a smaller community. A series of reports issued by CRS (Reese, 2003) focused on the cost of threat-level changes, but went deeper into the effects HSAS had on local communities regarding the vague warnings with no specific recommendations provided.

Agency was kept under an elevated threat for years despite knowing the true nature or potential targets of the threat. This situation was of minor impact in a city the size of Agency with no industry and not being a transportation hub. However, the lack of confidence and misunderstanding of HSAS was evident in Agency, as much as anywhere else. On visits home, friends and relatives would approach the author, ask what a specific threat meant, what they were suppose to do if it increased, and did it really apply to them. All they wanted to do was go about their normal daily routines without fear of a constant terrorist threat being broadcast before them in a system they no longer trusted or understood.

While developing a system that would fit every city equally would be near impossible, an effective advisory system would have flexibility to account for differences in population, geography, and transportation. The system should not instill fear or anxiety into the population, nor overtax the local economy while providing an effective shield against terrorist activity. HSAS was not the right fit as it provided little flexibility for cities to adjust. In addition, with NTAS being untested, no current method of knowing

how it would fit two such diverse locations exists. What is known is that by considering military installations as cities unto themselves, the DoD FPCON system does provide the type of flexible response sought.

VII. NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)

On July 14, 2009, Secretary Napolitano established the Homeland Security Advisory System Task Force to conduct a 60-day review of HSAS. Its mission was to assess effectiveness of the system in informing the public about terrorist threats and communicating protective measures within government and the private sector. The Task Force was co-chaired by Fran Townsend, former Assistant to President George W. Bush for Homeland Security, and Judge William Webster, former director of the Federal Bureau of Investigation and Central Intelligence Agency (Homeland Security, 2009a). In establishing this task force, Secretary Napolitano stated, "My goal is simple: to have the most effective system in place to inform the American people about threats to our country" (Homeland Security, 2009b).

In September 2009, the task force published its report and recommendation that included six major themes in the Executive Summary (Homeland Security Advisory Council, 2009a).

A. ENDURING MERIT OF A DEDICATED TERRORISM ADVISORY SYSTEM

The Task Force viewed a requirement for a threat warning system and that the system should be dedicated to terrorism. It found that significant work was warranted concerning providing useful and credible information to the general public along with improvements to government and the private sector. With the loss of public confidence, the Task Force recommended specific measures that should be taken including reducing the number of threat levels and that the system should be automatically lowered back to a baseline unless credible intelligence indicated remaining at a higher alert. Specific protocols were also recommended for the decision-making and communication process of changing a threat level (Homeland Security Advisory Council, 2009a).

B. TWO AUDIENCES—THE PUBLIC AND "INSTITUTIONS"

The Task Force agreed HSAS had two primary audiences. The first, consisting of the federal government, state and local governments, and the private sector, have used

HSAS for planning and has functioned reasonably well for this audience; however, improvements are needed. In regards to the second audience, the general public, the Task Force found that communication of useful information in a credible manner was poor and that significant work was warranted (Homeland Security Advisory Council, 2009a).

C. THE CURRENT ADVISORY SYSTEM—COMMANDING INSUFFICIENT PUBLIC CONFIDENCE

The Task Force agreed that, at best, indifference was directed at HSAS, with, at worst, a disturbing lack of public confidence in the system. The Task Force determined this situation must be remedied and outlined constructive measures divided into two topics, The Question of Colors and Measures to Restore Public Confidence (Homeland Security Advisory Council, 2009a).

As to maintaining a color-coded system, the Task Force was divided with half the membership believing the color-coded alerts were sufficiently clear, powerful, and easily understood and should be retained. The other half of the membership believed the color-coded system suffered from a lack of credibility and clarity leading to the erosion of public confidence and should be abandoned. All agreed that if retained, substantial reform was required (Homeland Security Advisory Council, 2009a).

To restore confidence in the system, the Task Force recommended the following measures to the Secretary (Homeland Security Advisory Council, 2009a).

- A discipline of more narrowly targeting the specific region and sector under threat, avoiding elevating the alert status of the nation as a whole.
- A practice of providing more specific information on new threats: including information on the type of threat, the credibility of the source of the information, and the steps the government is taking to mitigate the vulnerability.
- A practice of accompanying new alerts with actionable steps the public can take.
- An acknowledgement that the new baseline for the United States is guarded. This country remains a nation confronting the threat of terrorist attack, but given that it remains ever on guard, the number of levels can be reduced from five to three.

- As disciplined a focus on lowering the alert status as now goes into raising it.
- A practice of debriefing the nation after alerts have been issued—what happened to the threat, is it possible to now return to "guarded" status?

D. CHANGING THE ALERT LEVEL BASELINE TO GUARDED STATUS

In the judgment of the Task Force, a central feature of HSAS was that the threat level moved up more easily than it moved down. The Task Force stated a bias should exist against keeping the nation, region, or sector at an elevated alert in the absence of specific, ongoing threat information. They recommended the Secretary consider a "forcing mechanism" to return the level to "guarded" and that the alert level should be automatically lowered within 15 days unless credible intelligence indicated otherwise (Homeland Security Advisory Council, 2009a).

E. GREATER PRECISION IS REQUIRED IN IDENTIFYING THE SPECIFIC LOCAL GOVERNMENTS, FIRST RESPONDERS AND PRIVATE-SECTOR COMPANIES THREATENED AND THE PROTECTIVE MEASURES THAT NECESSITATE A RESPONSE

The Task Force recognized the significant success HSAS has had in the detailed planning of protective measures to be taken based on increased threats. It acknowledged the extensive planning and communication between thousands of agencies in developing response plans and recognized the role HSAS, as an instrument of national planning, contributed to this nation's enhanced state of readiness. However, the Task Force believed the cost in dollars of overly broad alerts is a substantial problem and recommended the following responses (Homeland Security Advisory Council, 2009a).

- Targeted raising of the formal alert status—as opposed to issuance of broad based verbal warnings.
- To the extent possible, the American people should be provided as much threat detail consistent with national security—with a focus on specific location and sector at actual risk.
- The alert system must return any elevated status to "guarded" as soon as possible, consistent with the threat intelligence, unless credible intelligence shows a need to maintain an elevated alert.

F. THE HOMELAND SECURITY ALERT SYSTEM WILL REQUIRE DEDICATED INFRASTRUCTURE, STAFF, ESTABLISHED PROTOCOLS AND PROCEDURES

HSAS was created during a crisis with admirable speed in the aftermath of 9/11. As a result, executive branch leaders responded to a rapid succession of threats using ad hoc practices for changing the nation's alert status and communicating the message. The system also had no staff dedicated to manage the work. The Task Force recommended the Secretary establish protocols, procedures, and staff with a basic infrastructure including the following (Homeland Security Advisory Council, 2009a).

- Criteria for deciding when an alert shall be made or a change in threat status announced
- A protocol for applying the criteria to new threat information
- A protocol for consultation with the White House
- A protocol for communicating alerts and new status information
- A protocol for providing the supporting information to the public at the time of the alerts
- Individuals designated to coordinate the resulting communications

In their report, the Task Force included a summary of 141 public comments concerning alteration of HSAS. Of these comments, 82 percent were in favor of replacing or altering HSAS, with a significant number in favor of scrapping the system altogether, while 16.5 percent recommended moving from colors to numbers, 11 percent favored scrapping the system and replacing it with words/alerts, while 5 percent favored changing to a stoplight-based color system. Only 18 percent offered support for HSAS (Homeland Security Advisory Council, 2009a).

Of those favoring change, the most common critique was based on colors, while many felt that HSAS used fear tactics and the system laced credibility due to its ambiguity. Concern of political manipulation and the need to infuse more specific information were voiced by most respondents. Reducing to three colors or incorporating a numerical scale with associated wording were also popular comments. Many felt the system lost its credibility when the whole nation was alerted while the threat was regional in nature. Of those expressing a desire to retain HSAS, the most common argument was

the amount of planning and measures already developed to align with the system would be wasted if a new system were implemented (Homeland Security Advisory Council, 2009a).

Based on the recommendations of the Task Force, Secretary Napolitano announced implementation of NTAS on April 20, 2011, by stating, "The terrorist threat facing our country has evolved significantly over the past ten years, and in today's environment….we know that the best security strategy is one that counts on the American public as a key partner in securing our country." She continued to state, "NTAS will provide the American public with information about credible threats" (Homeland Security, 2011d). Secretary Napolitano stated, "The old warnings using the color-coded system and indicating levels ranging from low to severe were too vague, the colors were there, but there was no information backing them up." She further stated, "the normal status for the country is high risk" (Fox News, 2011). It is interesting to note this statement, which in effect meant the conditions this nation had been living under were now the new baseline.

NTAS alerts will only be issued when credible information is available and will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat. Alerts will be based on the nature of the threat and are defined as the following (Homeland Security, 2011c).

- Elevated Threat—Warns of a credible terrorist threat against the United States
- Imminent Threat—Warns of a credible, specific, and impending terrorist threat against the United States

Dependent on the nature of the threat, alerts may be sent to law enforcement, distributed to affected areas of the private sector, or issued broadly to the public through official and social media channels, including the DHS webpage, Facebook, and Twitter (Homeland Security, 2011d).

An additional aspect of NTAS is the inclusion of a sunset provision indicating a specific time period when the alert will automatically expire unless new information becomes available warranting extension or if the threat itself evolves (Homeland Security, 2011d).

In her implementation remarks, Secretary Napolitano noted no current threats would reach the level to warrant one of the new alerts. Other remarks concerning NTAS were delivered by Representative Peter King of New York who "praised the new system as an upgrade that enhances current security efforts;" however, Senator Susan Collins of Maine cautioned that the new system must "effectively disseminate threat information in a timely manner and provide sound guidance to the public and affected homeland security partners on the actions they should take to protect themselves and the nation" (CNN Travel, 2011).

Representative Bennie Thompson of Mississippi issued a statement following the unveiling of NTAS, "Today marks an end to the era of color-coded scare tactics….because it failed to provide specific, actionable information….led to charges of manipulation to sow fear and gain political advantage and that the system being launched today promises credible information that members of the public can use to prepare, protect and respond" (Yahoo News, 2011a).

Despite lofty goals and the promise of how NTAS would restore credibility that had been lost under HSAS by providing information to the public regarding credible threats, in reality, a non-transparent system was created that has yet to issue an alert. NTAS not only replaced the color-coded HSAS, but it has also become invisible. The media has not asked any questions or opened discussions regarding NTAS, even during events that would seemingly call for an alert to be issued. While no metrics are available to determine the effectiveness of NTAS, it would be safe to say it has not performed as described since no alerts have been issued. The general public has little information about NTAS and has not had confidence restored in threat advisories since it has not been used. Restoring credibility has to be done by showing how the system works and providing credible threat information, not by placing it on a shelf and never using it.

VIII. OPTIONS

HSAS is broken, has lost credibility with the public, and with identified flaws, needs a revision or replacement advisory system to alert the public in a timely manner with credible information on terrorist activities. Critics of HSAS have charged the system is being used for political purposes and is failing to tell the public the whole story. Flaws identified in the beginning had yet to be addressed. The Task Force established to review HSAS came to similar conclusions and made several recommendations on repairing or replacing the system while remaining split on many issues. Secretary Napolitano chose to replace HSAS with NTAS as the best method to restore credibility.

Based on the author's research and understanding of HSAS, he reached similar options as the Task Force but with a different recommendation.

A. LEAVING HSAS IN PLACE

Keeping HSAS in place is no longer a viable option. Put into place in the aftermath of terrorist attacks, HSAS served its designed purpose, but quickly became overrun with criticism regarding the lack of information and political use. Usage of the system began to lapse as credibility faltered. With outlined flaws from GAO and CRS, along with the overall negative opinion of HSAS, keeping the system in place would be a difficult task. A complete revision of HSAS and its processes would be required to restore integrity and trust.

Research was conducted to see if HSAS could be improved by implementing processes from comparable international systems; however, after reviewing the few systems in place, it was determined they had similar flaws or would be even more difficult for individuals to understand than HSAS.

In reviewing state homeland security websites to see how information was being posted, or how security procedures were being recommended for the varying threat levels, some states had no reference at all to HSAS, to include the current threat condition

level, other than a link to the DHS website. The trend in several states was towards an all hazards approach in developing preparedness and response plans that lumped terrorism in with natural disasters, which HSAS had not been designed to achieve.

When Secretary Napolitano established the Homeland Security Advisory System Task Force to conduct a review of HSAS, the picture began to clear. The findings of the Task Force indicated major changes were required to establish a system that would be effective and found trustworthy.

B. REPLACING HSAS WITH THE NATIONAL TERRORISM ADVISORY SYSTEM (CURRENTLY IMPLEMENTED)

NTAS is currently the alert system in place. Its intended purpose is to keep the U.S. populace informed of credible terrorist threats. Secretary Napolitano announced implementation of the NTAS on April 20, 2011 based on recommendations from the Task Force. The color-coded system and vague information were now gone and replaced by terrorist alerts. Despite the country being placed at "High Risk," it was noted no current threats existed that would reach the level to warrant one of the new alerts. NTAS alerts will only be issued when credible information is available and will provide a concise summary of the threat along with information about actions to be taken to help prevent, mitigate, or respond to the threat.

Almost two years have passed, and no NTAS alerts have been issued regarding terrorist threats. Terrorist activity, or the threat of such activity, has occurred during this time frame. Either the information was not deemed credible, did not reach the level required to issue an alert, or was not issued for political reasons. It is unfortunate that the system put into place to restore credibility and public confidence has not been used to do just that. It is almost as if the new system itself has become non-existent. NTAS has never been practiced nor has the media discussed it, and the author ventures the majority of the public knows little or nothing about the alerts. If this system is going to be retained, it needs to be utilized so that the public is made aware of what to expect and how to respond.

C. MERGING HSAS WITH THE DEPARTMENT OF DEFENSE FPCON

A third option would be to merge HSAS with DoD FPCON. While not complementary to each other, the two systems have the same functions and are closely enough related that a merger of the two would provide a revised system with credibility and ease of understanding. The color-coding could be brought along and associated with the FPCON levels.

While the process would be fraught with concern over military control and allegations of further government intrusion, merging HSAS with DoD FPCON would provide an easily recognized system that a large portion of the population (having served, worked, or lived on military installations) would understand. As previously shown in Figures 6 and 7, HSAS vs. FPCON Levels, the FPCON system aligns with HSAS in regards to threat level definitions although not specifically designed to complement.

The process for instituting a change in threat level would not be any different and the system could be used locally for regional threats or nationally. The duration of the threat alerts would be minimized as the FPCON system was not designed to be maintained at high alert levels for long periods of time. An advantage of the FPCON system is that it already possesses pre-designed measures to be taken to improve security that could easily be adapted for use by other federal agencies.

Military installations also prominently post FPCON at the gates and on buildings to remind personnel of the threat nature, a practice in which the public no longer engages as the aspect of terrorism is being removed from view; hence, the lack of alerts under NTAS. Other countries are not shy about posting information on terrorist threats and make it accessible on unclassified websites. While it is possible to access the DHS website and find information about NTAS, references to terrorist activity are not to be found.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. DISCUSSION

A. CONCLUSIONS

When this thesis was begun, the argument was that HSAS needed to be repaired or replaced with an alternative system. HSAS was implemented six months after the attacks of 9/11. The system was coordinated and thought out before implementation. However, with the urgency to implement a system, basic flaws were subsequently identified in GAO and CRS reports discussed in this thesis. In addition to the government reports, many critics of the system broached concerns of political manipulation and scare tactics by raising alerts without providing appropriate information to the public. With the decline of public acceptance of HSAS, leaving the system in place as is was not a viable option, although except for airports, it was almost out of the public conscience after the last revision in August 2006 and may have eventually faded away on its own.

HSAS served its purpose and brought this nation through the immediate response to 9/11, but the financial and psychological costs of maintaining a constant high alert were rapidly draining available resources. Whatever was done to revise the system needed to ensure the threat system maintained credibility, relied on credible intelligence, had actionable measures to take, and was easily understood by the general population. Whether it remained focused as a system primarily for federal agencies, or revised with state and local governments along with private industry, is a question that must be raised particularly with state and local governments, as well as industry developing their own measures or ignoring terrorist activity in their public response plans. Consideration of where HSAS failed in providing information to the public needs to be improved with technology and supplying the public with responses to questions when the system was used. The information on HSAS supports the fact that revisions were required to maintain credibility of the terror alert system.

However, as often happens when projects begin, circumstances can change the landscape and new factors are brought into play that impact the decision process. In this case, the delay in completing this thesis allowed time for DHS to establish a task force,

review HSAS, and make recommendations on how to improve the system. The ultimate result was the implementation of NTAS to replace HSAS. The Task Force's work and subsequent development of NTAS sustained the argument that HSAS was flawed and required changes. NTAS remains untested and needs more time to see how it functions during crises and for potential critics to review the decisions made when altering the threat level.

Now that NTAS is being used, not surprisingly, very little seems to have changed, other than NTAS is not in the spotlight of the media or comedians as HSAS tended to be. The military installations in San Antonio are currently at FPCON Alpha, which is still a step below the wording of NTAS. Individuals are still taking the same precautionary measures they had become accustomed to under HSAS. At least that is how it appears. Upon closer examination, the measures had become so ingrained that the mere changing of words and elimination of a color had not changed processes, but had placed the public in a different level. Following implementation of NTAS, it was naturally taken for granted the country was operating under the old Yellow (Elevated Alert) and maintained the routines that had been established. However, if that were true, what happened to the Orange Level (High Alert) that had been in place at the airports? During the switch from HSAS to NTAS, no discussion of a change in the threat level occurred, just that the announcements and color codes were missing in the terminals.

Look back at the statement made by Secretary Napolitano when she stated, "the normal status for the country is high risk" (Fox News, 2011). It was subtle, but it did appear in the wording, "high risk," which under HSAS, was equivalent to Orange, and was now classified as the normal daily status while "elevated," the next step in alerts under NTAS, had been the normal status for years under HSAS. It was a subtle change; the colors were eliminated, the wording changed, and the same security measures kept in place.

The anniversary of 9/11 came around with the expectation of seeing multiple alerts issued under NTAS. No alert was issued to the news media or through the social network sites, Twitter and Facebook, although credible threats were being reported and the DoD FPCON was elevated to Bravo. If reports were flowing from fusion centers

through law enforcement channels and appropriate measures were taken against terrorist activity, the general public was not informed. This situation is of significant concern as NTAS was designed to provide transparency, and was touted as more open in providing information to the public than its predecessor. NTAS may in fact be utilized as a terrorist threat advisory alert even less than HSAS.

It appears as if the problem-plagued color-coded HSAS was replaced with an invisible NTAS that for all intent and purposes could probably disappear without the general public even noticing. Maybe the intent was to have an unseen system, but with less information disseminated on NTAS than under HSAS. The concern to the general public will be the ability to understand an increased level if one is ever announced. With no usage to support or critique NTAS, its effectiveness is difficult to evaluate. While NTAS has quieted public concern about threat levels, it also has not fully lived up to its expectations of sharing information on threat activity.

Although not directly linked to DoD FPCON, a close enough relationship exists with HSAS that they could be linked to provide a true nationwide terrorist alert system. The FPCON level and terrorist threat, based on the same intelligence and removed from the political arena, should tell the same story to the general public, as well as government agencies. Regardless of the system that will be used in the future, it should be designed and implemented to not be done in a manner that would compromise security or response to a terrorist attack. The UK Threat Level System is a good example to follow. After the London subway bombings, MI-5 made its system accessible to the public at an unclassified level. Not only does it address the threat level, it also discusses in detail the source and form of the threat, both internationally and domestically. The United States seem to have gone the other way in the last few years and made this nation's system less public friendly.

B. RECOMMENDATION

A merger of HSAS with DoD FPCON would repair the lost credibility and revitalize the terrorist threat alert process. The two systems are similar in nature, although HSAS was not designed to complement the FPCON system. The easy color-coding

recognition of HSAS combined with the threat levels and established measures in the FPCON system are a match that should be implemented to provide federal agencies, the industrial sector, and the general public with the best threat advisory system.

A new Task Force, similar to the one that studied HSAS, should be formed to review the effectiveness of NTAS, and ascertain why, after two years, no alerts have been issued. As part of this study, it should determine the requirement for a terrorist advisory system and the public's desire to be provided with information. Again, the UK system would be a good example to follow on how information is displayed and presented for the public.

As the struggle against terrorism continues, U.S. advisory systems need to adapt, be credible, and flexible enough to meet all situations, which DoD FPCON has done over time, and should be adopted across all federal agencies as a common threat advisory system and run jointly by DHS and USNORTHCOM. The industrial sector should be encouraged to adopt similar measures along with state homeland security offices, from where it would trickle down to the public. Eventually, the result will be one common easily understood alert system that will restore public confidence.

LIST OF REFERENCES

ABC News. (2011). *Terror alert color code fades to black: New threat warning system coming online.* Retrieved from http://abcnews.go.com/US/terror-alert-color-code-fades-black-threat-warning/story?id=13414402

Air Force Manual 10-100. (2004, June 1). *Force protection condition*.

Absolute Astronomy. (2008). *Vigipirate*. Retrieved from http://www.absoluteastronomy.com/topics/Vigipirate

Alaska Department of Military and Veterans Affairs. (2002). *Threat levels*. Retrieved from http://www.ak-prepared.com/dmva/threat_levels.htm

Alaska Division of Homeland Security and Emergency Management. (2008). *Elevated threat level procedures (draft).* Retrieved from http://www.ak-prepared.com/homelandsecurity/threat_elevated.htm

American Red Cross. (2003). *Red cross homeland security advisory system recommendations.* Retrieved from http://www.redcross.org/article/0,1072,0_1_1418,00.html

Archick, K., Ek, C., Gallis, P., Miko, F., & Woehrel, S. (2006, July). *European approaches to homeland security and counterterrorism* (Congressional Research No. RL33573). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: www.fas.org/sgp/crs/homesec/RL33573.pdf

Asis International. (2008). *Threat advisory system response guidelines*. Retrieved from www.asisonline.org/guidelines/guidelinesthreat.pdf

Bessonov, K. (2008). Color-coded terror threat system to guard Russia. Retrieved from Moscow News Weekly website: http://mnweekly.ru/news/20080313/55316888.html

Bush, G. (2002). *Homeland security presidential directive-3*. Retrieved from The White House website: http://www.whitehouse.gov/news/releases/2002/03/print/20020312-5.html

Bush, G. (2003). *Homeland security presidential directive-5*. Retrieved from The White House website: http://www.whitehouse.gov/news/releases/2003/02/print/20030228-9.html

Center for Defense Information Terrorism Project. (2002). *Terror alerts: The homeland security advisory system*. Retrieved from http://www.cdi.org/terrorism/alerts.cfm

Chertoff, M. (2006, August). *Statement by homeland security secretary Michael Chertoff announcing a change to the nation's threat level for the aviation sector*. Retrieved from Department of Homeland Security website: http://www.dhs.gov/xnews/releases/pr_1158349923199.shtm

CNN Travel. (2011). *New terrorism alert system will offer specific warnings.* Retrieved from http://articles.cnn.com/2011-04-20/travel/terrorism.advisory.system_1_alert-levels-terrorist-threat-warnings?_s=PM:TRAVEL

Colorado Division of Emergency Management. (2008). *Homeland security*. Retrieved from http://www.dola.state.co.us/dem/homeland_security/homeland_security.htm

Commonwealth of Pennsylvania Office of Homeland Security. (2002). *HSAS information, homeland security advisory system (HSAS) threat condition*. Retrieved from http://www.homelandsecurity.state.pa.us/homelandsecurity/cwp/view.asp?a=437&q=148361

Continuity Central. (2011). *Implementation of US national terrorism advisory system announced.* Retrieved from http://www.continuitycentral.com/news05708.html

Department of Defense Instruction (DoDI) 2000.16. (2006, October 2). *DoD antiterrorism standards*. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf

EAA News. (2011). *New national terrorism advisory system unveiled.* Retrieved from http://www.eaa.org/news/2011/2011-04-21_advisories.asp

Fox News. (2011). *New terror alerts will be specific and short lived, Napolitano says.* Retrieved from http://www.foxnews.com/politics/2011/04/20/new-terror-alerts-specific-short-lived-napolitano-says/

General Accounting Office. (2004a). *Homeland security advisory system: Preliminary observations regarding threat level increases from yellow to orange*. (GAO-04-453R). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d04453r.pdf

General Accounting Office. (2004b). *Homeland security communication protocols and risk communication principles can assist in refining the advisory system* (GAO-04-682). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d04682.pdf

Governor's Office of Emergency Services. (2003). *California state agency guidance: Homeland security advisory system*. Retrieved from www.oes.ca.gov/Operational/OESHome.nsf/PDF/HomelandSecGuide/$file/HomelandSecGuide.pdf

Homeland Security. (2008a). *Chronology of changes to the homeland security advisory system*. Retrieved from http://www.dhs.gov/xabout/history/editorial_0844.shtm

Homeland Security. (2008b). *Homeland security advisory system*. Retrieved from http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

Homeland Security. (2009a). *Homeland security advisory system task force*. Retrieved from http://www.dhs.gov/files/committees/gc_1247517287253.shtm

Homeland Security. (2009b). *Secretary Napolitano announces 60-day review of homeland security advisory system*. Retrieved from http://www.dhs.gov/ynews/releases/pr_1247586668272.shtm

Homeland Security. (2011a). *National terrorism advisory system*. Retrieved from http://www.dhs.gov/files/programs/ntas.shtm

Homeland Security. (2011b). *NTAS frequently asked questions*. Retrieved from http://www.dhs.gov/files/publications/ntas-questions-answers.shtm

Homeland Security. (2011c). *NTAS public guide*. Retrieved from http://www.dhs.gov/files/publications/ntas-public-guide.shtm

Homeland Security. (2011d). *Secretary Napolitano announces implementation of national terrorism advisory system*. Retrieved from http://www.dhs.gov/ynews/releases/pr_1303296515462.shtm

Homeland Security. (2011e). *Secretary Napolitano announces new national terrorism advisory system to more effectively communicate information about terrorist threats to the American public*. Retrieved from http://www.dhs.gov/ynews/releases/pr_1296158119383.shtm

Homeland Security. (2011f). *The blog @ homeland security: The new national terrorism advisory system*. Retrieved from http://blog.dhs.gov/2011/04/new-national-terrorism-advisory-system.html

Homeland Security Advisory Council. (2009a). *Homeland security advisory system task force report and recommendations*. Retrieved from http://www.dhs.gov/xlibrary/assets/hsac_final_report_09_15_09.pdf

Homeland Security Advisory Council. (2009b). *HSAS task force stakeholder feedback.* Retrieved from U.S. Department of Homeland Security website: http://www.dhs.gov/xlibrary/assets/hsas_task_force_stakeholder_feedback.pdf

Homeland Security Advisory System Task Force. (n.d.). *Summary of public comments made on the homeland security advisory system*. Retrieved from U.S. Department of Homeland Security website: http://www.dhs.gov/xlibrary/assets/hsas_summary_of_public_comments.pdf

Homeland Security Brief. (2003, August). *Color-coding security: State homeland security advisory systems*. Retrieved from The Council of State Governments website: http://www.csg.org/pubs/Documents/Brief0703ColorCodingSecurity.pdf

Homeland Security Press Release. (2006, August). *DHS adjusts threat level from red to orange for in-bound flights from the UK*. Retrieved from U.S. Department of Homeland Security website: http://www.dhs.gov/xnews/releases/pr_1156517870332.shtm

Iowa Homeland Security and Emergency Management. (2008). *About Iowa homeland security and emergency management*. Retrieved from http://www.iowahomelandsecurity.org/AboutUs/HSEMD/tabid/55/Default.aspx

Intellnet. (2003). *France sets up new terror alert system based on color codes*. Retrieved from http://www.intellnet.org/news/2003/03/27/18689-1.html

Joint Publication (JP) 3-07.2. (1998, March 17). *Joint tactics, techniques, and procedures for antiterrorism, appendix J: THREATCON system*. Retrieved from The Air University website: http://www.au.af.mil/au/awc/awcgate/jp/jp3_07_2.pdf

Kemp, R. L. (2005, October). Homeland security: Common-sense measure to safeguard your community, *Public Management*, *87*(9), 34–35. Retrieved from Naval Postgraduate School Dudley Knox Library website: http://libproxy.nps.edu/login?url=http:search.ebscohost.com/login.aspx?direct=true&db=bth&AN=18419007&site=ehost-live&scope=site

McDermott, R., & Zimbardo, P. (2007). The psychological consequences of terrorist alerts. In B. Bongar, L. M. Brown, L. E. Beutler, J. N. Breckenridge, & P. G. Zimbardo (Eds.), *Psychology of terrorism* (pp. 357–370). New York, NY: Oxford University Press.

National Coordinator for Counterterrorism (NCTb). (2008). *Current threat levels for the Netherlands*. Retrieved from http://english.nctb.nl/what_is_terrorism/Current_threat_level/index.aspx

National Counter-Terrorism Committee. (2005). *National counter-terrorism plan*. Retrieved from Australian Government Attorney-General's Department website: http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/85A16ADB86A23AD1CA256FC600072E6B?OpenDocument

National Counter-Terrorism Committee. (2008). *National security public information guidelines*. Retrieved from http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~8NSPIGLET_Public.pdf/$file/8NSPIGLET_Public.pdf

Nebraska Emergency Management Agency. (2008). *Homeland security*. Retrieved from http://www.nema.ne.gov/index_html?page=content/home_news/homelandsecurity_home.html

North American Electric Reliability Council (NERC). (2002a). *Electricity sector comments on the homeland security advisory system (attachment to letter from NERC president Michehl Gent to federal bureau of investigation director Robert Mueller).* Retrieved from www.nerc.com/docs/cip/ESCommentsonHSAS.pdf

North American Electric Reliability Council (NERC). (2002b). *Threat alert system and physical response guidelines for the electricity sector (version 2).* Retrieved from www.iwar.org.uk/infocon/threat-levels/tas_physical_V2.pdf

North American Electric Reliability Council (NERC). (2005, November). *Security guidelines for the electricity sector (version 3).* Retrieved from www.esisac.com/publicdocs/Guides/SecGuide_PhysResponse_BOTapprvd1Nov2005.pdf

North Dakota Department of Emergency Services. (2008). *Homeland security*. Retrieved from www.nd.gov/des/homeland/

Online.com. (2011). *Advisory system replaces color-coded terror alerts*. Retrieved from http://www.cnjonline.com/news/system-42973-alert-advisory.html

Online NewsHour. (2003). *Domestic security: The homefront and the war on terrorism*. Retrieved from http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/hsas.html

ProjectDisaster.com. (2011). *Secretary Napolitano announces implementation of national terrorism advisory system*. Retrieved from http://projectdisaster.com/?p=38888

Reddick, C. (2007, September). Homeland security preparedness and planning in U.S. city governments: A survey of city managers, *Journal of Contingencies and Crisis Management*, *15*(3), pp. 157–167. Retrieved from Naval Postgraduate School Dudley Knox Library website: http://libproxy.nps.edu/login?url=http:search.ebscohost.com/login.aspx?direct=true&db=bth&AN=25944941&site=ehost-live&scope=site

Reese, S. (2003, August). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps21-012606-01.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2004a). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Retrieved Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps10-110504-09.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2004b). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps08-120904-05.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2005a). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps18-020705-06.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2005b). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Retrieved Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps18-040105-06.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2006, December). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps03-011807-11.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2007, March). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps35-040507-05.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Reese, S. (2008, January). *Homeland security advisory system: Possible issues for congressional oversight* (Congressional Research No. RL32023). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: https://www.hsdl.org/homesec/docs/crs/nps30-022008-02.pdf&code=37aac360be81fd5bd5473ff9ded7fa1e

Security Service MI5. (2008). *The UK's threat level system*. Retrieved from http://www.mi5.gov.uk/output/Page26.html

Schmidt, D. (2004, June/July). The homeland security advisory system: Providing a framework for business security, *Remote Site & Equipment Management Magazine*. Retrieved from www.remotemagazine.com/images/MarshJune04.pdf

Security Products. (2011). *National terrorism advisory system implemented*. Retrieved from http://secprodonline.com/articles/2011/04/21/national-terrorism-advisory-system-implemented.aspx?sc_lang=en

Shapiro, J., & Cohen, D. (2007, Fall). Color blind, lessons from the failed homeland security advisory system. *International Security*, *32*(2), 121–154. Retrieved from Naval Postgraduate School Dudley Knox Library website: http://muse.jhu.edu.libproxy.nps.edu/journals/international_security/v032/32.2shapiro.html

Sordo, F. N. (2006, December 9). Europe's anti-terror alert systems are out of tune with each other. *The European Magazine*. Retrieved from http://www.cafebabel.com/eng/article/18024/europes-anti-terror-alert-systems-are-out-of-tune-.html

South Dakota Office of Homeland Security. (2008). Retrieved from www.state.sd.us/homeland/

ThomasNet News. (2011). *New national terrorism advisory system goes into effect.* Retrieved from http://news.thomasnet.com/companystory/New-National-Terrorism-Advisory-System-goes-into-effect-595305

UK Intelligence Community Online. (2008). *Threat levels: The system to assess the threat from international terrorism*. Retrieved from http://www.intelligence.gov.uk/threat_levels.aspx

U.S. Census Bureau. (2010a). *U.S. census bureau releases data on population distribution and change in the U.S. based on analysis of 2010 census results*. Retrieved from http://2010.census.gov/news/releases/operations/cb11-cn124.html

U.S. Census Bureau. (2010b). *2010 census interactive population search*. Retrieved from http://2010.census.gov/2010census/popmap/ipmtext.php?fl=19

U.S. Census Bureau. (2011). *U.S. census bureau delivers Texas' 2010 census population totals, including first look at race and Hispanic origin data for legislative redistricting*. Retrieved from http://2010.census.gov/news/releases/operations/cb11-cn37.html

USNORTHCOM News. (2007). *USNORTHCOM sets force protection level for military installations*. Retrieved from http://www.northcom.mil/News/2007/070307.html

Utah Department of Public Safety. (2008). *Division of homeland security*. Retrieved from http://publicsafety.utah.gov/homelandsecurity/index.html

The White House Blog. (2011). *The new national terrorism advisory system*. Retrieved from http://www.whitehouse.gov/blog/2011/04/20/new-national-terrorism-advisory-system

White House. (2002a). *Remarks by governor Ridge at announcement of homeland security advisory system* [Press release]. Retrieved from http://www.whitehouse.gov/news/releases/2002/03/20020312-11.*html*

White House. (2002b). *Director Ridge, attorney general Ashcroft discuss threat level* [Press release]. Retrieved from http://www.whitehouse.gov/news/releases/2002/09/20020910-5.html

Wyoming Office of Homeland Security. (2008). *Being prepared*. Retrieved from http://wyohomelandsecurity.state.wy.us/being_prepared.aspx

Vigipirate. (2008). In *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Vigipirate

Yahoo News. (2011a). *New terrorism advisory system promises credible information for public*. Retrieved from http://news.yahoo.com/s/usnw/20110420/pl_usnw/BX86967

Yahoo News. (2011b). *US to use facebook, twitter to issue terror alerts*. Retrieved from http://news.yahoo.com/s/ap/20110407/ap_on_re_us/us_color_coded_threats

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California