

Current HSAS Condition as of
March 31, 2002.



Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper



www.wmdtaskforce.com



www.bulwarkz.com

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

Table of Contents

SECTION	PAGE
Introduction	2
Security Advisory System (<i>Explained</i>)	3
- National Framework	
- Factors for Assignment for National ThreatCON	
- Unified System for Public Announcements	
- ThreatCON Levels	
o Green	
o Blue	
o Yellow	
o Orange	
o Red	
Cyber Security and Cyber Terrorism	7
Personnel Security Threats	8
Physical Security Threats	9
Policies and Procedures	9
Hazardous Materials Security (<i>HAZMAT Security</i>)	10
Liability for Organizations Targeted by Terror Attacks (<i>A Legal Perspective</i>)	11
Interfacing with Emergency Response Planners	12
<u>APPENDIX A</u>	
The Author's Biographical Information	13
<u>APPENDIX B</u>	
Presidential Directive – 3	17

Copyright © 2002 Bulwarkz Defensive Solutions and WMD Task Force. All Rights reserved.
This publication is protected by Copyright and international treaty. No part of this publication may be reproduced in any form by any means without prior written permission from Bulwarkz Defensive Solutions. This publication is provided "AS-IS" without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. **This document is not associated in any fashion with either the Executive Branch of the United States Government or the Office of the President of the United States of America, its' Associates or Directors.**

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

INTRODUCTION

What major concerns are government and corporate agencies facing regarding Homeland Defense Planning? Bulwarkz and WMD Task Force security professionals were recently asked to address the issues such organizations need to consider. Their main concern is how to determine if the major issues are being properly addressed. These basic points address multiple facets of a comprehensive Risk Management model.

In order to properly determine the appropriate level and type of investment in a comprehensive Homeland Defense Plan, it is essential to have a sound grasp of the probability and magnitude of damage that could occur from a Direct or Indirect Terrorist Act. If a terrorist event were to occur directly or indirectly against you or your organization, how would you address needed issues before the actual event occurs? Do you have a plan in place that is practiced and coordinated? Is your plan periodically updated to reflect changes within your organization? Are all your employees aware of this plan? Has this plan been coordinated with local emergency responders?

Unfortunately, unless you have the background and training in Counter Terrorism Planning, are familiar with Weapons of Mass Destruction and are addressing specific events that could potentially collapse your entire digital infrastructure (Cyber Terrorism), you, as with most organizations, are only brushing over the issues to which you are exposed.

Bulwarkz and the WMD Task Force realize there is a total lack of statistical or actuarial information addressing terrorist acts in North America. All that can be done is to address aspects of known activity throughout the world and apply those same principles and practices within our own environment.

Effective Homeland Defense Planning is a practice, and a mindset that is rapidly becoming a way-of-life for all Americans. Whether you hold a personal, financial or legal responsibility to your employees, stockholders or to your family, as a leader you would be severely remiss in your duties to not consider effective Homeland Defense Planning.

Why did WMD Task Force and Bulwarkz Defensive Solutions combine on this collaborative white paper? The expertise within the WMD Task Force focuses on Weapons of Mass Destruction (WMD), e.g., Nuclear, Biological, Chemical and Conventional weaponry. The expertise within Bulwarkz focuses on Technical security issues (Cyber Security and Cyber Terrorism) as they relate to TCP/IP based networks. Therefore, in order to address the many aspects of Homeland Defense Planning, it would be impractical for one organization to make a claim of having all the needed expertise. A collaborative effort ensures the client that they get the best expertise available.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

SECURITY ADVISORY SYSTEM (*Explained*)

National framework:

But, as I said before, we're asking all federal departments and agencies make this system work immediately, integrate their plans into this advisory system, and work with us over the next 135 days to a final system.

Governor Tom Ridge; Speech before the Nation on March 12, 2002

This system of alerting is designed as a National framework for federal, state, and local governments, private industry and the public. There are many federal alert systems in our country, each are tailored and unique to different sectors of our society: transportation, defense, agriculture, and weather are only some examples. These alert systems fill vital and specific requirements for a variety of situations in both the commercial and government sectors.

The Homeland Security Advisory System (HSAS) is designed to provide a national framework for a Terrorist Activity Alerting system. It allows government officials and citizens to communicate the nature and degree of terrorist activity. This advisory system characterizes appropriate levels of vigilance, preparedness and readiness in a series of graduated Threat Conditions. Each Threat Condition (ThreatCON) has a very general set of Protective Measures that correspond to each ThreatCON color and/or level. These protective measures will help the government and citizens decide what action needs to be taken to help counter and respond to terrorist activity. Based on the threat level, federal agencies will implement appropriate Protective Measures. States and localities will be encouraged to adopt their own compatible systems.

Factors for assignment of National ThreatCONs:

The Homeland Security Advisory System will provide a framework for the Attorney General, in consultation with the Director of the Office of Homeland Security, to assign ThreatCONs, which can apply nationally, regionally, by sector or to a potential target. Cabinet Secretaries and other members of the Homeland Security Council will be consulted as appropriate. A variety of factors may be used to assess the threat. These may include, but are not limited to:

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- How grave is the threat?

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

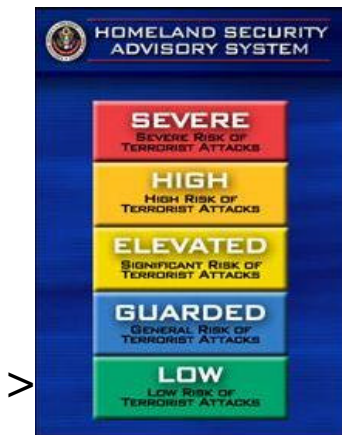
March 31, 2002

Unified system for public announcements:

Public announcements of threat advisories and alerts help deter terrorist activity, notify law enforcement and state and local government officials of threats, inform the public about government preparations, and provide them with the information necessary to respond to the threat. State and local officials will be informed in advance of national threat advisories when possible. The Attorney General will develop a system for expeditiously conveying relevant information to federal, state, and local officials as well as the private sector. Heightened ThreatCONs can be declared for the entire nation, a specific geographic area, functional or industrial sector. Changes in assigned Threat Conditions will be made when necessary.

ThreatCON Levels:

ThreatCONs characterize the risk of terrorist attack. Protective Measures are the steps that will be taken by the government and private sector to reduce vulnerabilities. The HSAS establishes five Threat Conditions with associated suggested Protective Measures:



Green Low Condition

Low risk of terrorist attacks.

The following Protective Measures may be applied:

- 1.) Refining and exercising preplanned Protective Measures;
- 2.) Ensuring personnel receive training on HSAS;
- 3.) Departmental or agency-specific Protective Measures; and
- 4.) Regularly assessing facilities for vulnerabilities and taking measures to reduce them.



Blue Guarded Condition

General risk of terrorist attack

In addition to the previously outlined Protective Measures, the following may be applied:

- 1.) Checking communications with designated emergency response or command locations;
- 2.) Reviewing and updating emergency response procedures; and
- 3.) Providing the public with necessary information.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

Yellow Elevated Condition

Significant risk of terrorist attacks.

In addition to the previously outlined Protective Measures, the following may be applied:

- 1.) Increasing surveillance of critical locations;
- 2.) Coordinating emergency plans with nearby jurisdictions;
- 3.) Assessing further refinement of Protective Measures within the context of the current threat information; and
- 4.) Implementing, as appropriate, contingency and emergency response plans.

Orange High Condition

High risk of terrorist attacks.

In addition to the previously outlined Protective Measures, the following may be applied:

- 1.) Coordinating necessary security efforts with armed forces or law enforcement agencies;
- 2.) Taking additional precaution at public events;
- 3.) Preparing to work at an alternate site or with a dispersed workforce; and
- 4.) Restricting access to essential personnel only.



Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

RED

Severe Condition



Severe risk of terrorist attacks.

***In addition to** the previously outlined Protective Measures, the following may be applied:*

- 1.) Assigning emergency response personnel and pre-positioning specially trained teams;
- 2.) Monitoring, redirecting or constraining transportation systems;
- 3.) Closing public and government facilities; and
- 4.) Increasing or redirecting personnel to address critical emergency needs.

If you have any specific comments about the Homeland Security Advisory System you can send them in writing to:

Director, Federal Bureau of Investigation
Homeland Security Advisory System, Room 7222
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535.

Or

[\(HSAScomments@fbi.gov\)](mailto:HSAScomments@fbi.gov)

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

CYBER SECURITY AND CYBER TERRORISM

Throughout our society it is easy to realize the full integration of automated data processing applications (computer software and hardware). These applications help us do many tasks, including scheduling our own airline flights, complex mathematic analysis, supporting our corporate infrastructure and sending emails to family and friends.

The information age that allows us to quickly gain Internet access to gather information, send email or make financial transactions also exposes us to the villains of the world. Therefore, as a government or corporate entity that uses the Internet to conduct business, our security concerns have now been exponentially increased.

Every major company in the world has an "Internet Presence." Their employees, customers and shareholders expect it. The Internet has become a significant aspect of our lives and is as important as our personal automobile. Just like this automobile has safety features, every company needs to ask themselves; does this Internet presence have the needed security measures? But more so how do we as consumers and citizens know if they do or do not?

These are tough questions companies are continually addressing. Now they have an added concern of Cyber Terrorism. With Cyber Terrorism, an Internet based attack can take various forms from a Distributed Denial of Service attack to a concentrated and focused effort to attempt a full network compromise. The devastating reality of a cyber attack is that it can occur from anywhere in the world.

The simple sobering fact is the Internet has brought the terrorist, who can be located in a far and distant land, right to our digital front door. In some instances, behind this digital front door are our bank account, our personal and very private medical information and our countries governmental and financial infrastructure.

Often simple and basic network security practices and concerns are ignored and overlooked in an effort to have a better bottom line or because it just has not been a concern within the organization. Organizations should ask themselves some basic questions:

- a.) Do I have properly configured perimeter security (Router & Firewall)?
- b.) Do I effectively monitor my network for breach attempts?
- c.) Do I have a response plan in the event I do detect a network breach?
- d.) Can I respond to a network breach?
- e.) Have I effectively analyzed where my network vulnerabilities are located?
- f.) Do I have a wireless aspect to my network and how secure is this wireless segment?

Cyber Terrorists do not have to break a window to gain access to you. They can sit in their living room in some distant land, in a relaxed and somewhat protected environment and exploit our infrastructure without the worry of repercussions. Simply, some foreign countries have little to no ability legally or technically, or the desire to actively pursue illegal cyber activities. You are on your own, so plan well!

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

PERSONNEL SECURITY THREATS

Protecting valuable human lives should be of highest priority for any organization given the indiscriminate attacks on military, political, economic, symbolic and psychological targets by terrorists. Your people and assets may become direct or indirect victims of attacks by nuclear, biological, chemical or conventional (NBC²) munitions. Within the area of a direct attack there will be mass destruction and loss of life, not to mention injuries to personnel in the surrounding areas. Biological and chemical weapons of mass destruction could present an indirect hazard to anyone within the downwind path of airborne contaminants. Most disaster response plans are based on our immediate concerns to fires and natural disasters (earthquakes, tornadoes, etc.). These disaster response plans have conditioned people on the proper procedures to take in the event one or more of these activities should they occur. State, local and federal government agencies, as well as most large companies, practice these procedures. This “conditioned response” could expose personnel to hazardous environments when weapons of mass destruction are involved.

Each type of NBC² weapon requires a different response:

- 1.) Is it safer to stay in the building and turn off the Heating, Ventilation and Air Conditioning (HVAC) system? *{Once the HVAC system is contaminated with Radiological debris (from a dirty nuclear bomb) it could force inadvertent exposure to people in an enclosed area.}*
- 2.) Should you move lower in the building to reduce exposure? *{Majority of the Biological Agents are lighter than air and tends to loft through the air moving higher into a structure.}*
- 3.) Should you move higher in the building to reduce exposure? *{For the most part Chemical Agents are heavier than air and tend to settle in basements or stairwells, therefore you should move higher in the structure.}*
- 4.) If there is a conventional weapon involved (i.e., a truck bomb) is there a secondary device and subsequent concern for any additional NBC exposure? *{Sometimes Terrorists use conventional munitions as a delivery vehicle for a secondary NBC type of weapon.}*

Depending on the probability or vulnerability of your facilities, you may have to institute different response plans and warning signals for each type of incident. The swirling clouds of smoke and dust from the World Trade Center are etched in our collective conscience. Just imagine if every dust particle in those clouds carried a radiological, chemical and/or biological contaminant, the casualties would have been exponentially greater. Planning responses and practicing drills are preventive measures you can do today to reduce the vulnerability and liability of your organization.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

PHYSICAL SECURITY THREATS

The threat to facilities and critical infrastructures are staggering considering that terrorists have no reservation in sacrificing their own lives. Explosive devices in vehicles or carried by people can create a significant incident if you allow them access to your facilities. So, how do you keep the bad guys away and not cripple your organization? Here are some quick suggestions to help you consider reducing your vulnerability:

- Install security systems that only allow authorized personnel access.
- Limit access points.
- Screen visitors and deliveries away from critical structures or functions.
- Monitor the arrival and departure of visitors.
- Limit parking and access of vehicles close to structures.
- Eliminate high-speed avenues of approach by installing barriers altering vehicle traffic flow patterns.

Your vulnerability must be assessed through the eyes of a terrorist. Obtain an “outside looking in” view of your organization and facilities.

POLICIES AND PROCEDURES

Leaders throughout our communities, corporations and organizations must be proactive in establishing policies and procedures to deal with a catastrophic event in or near their facilities. Vigilance and deterrence are essential elements in changing the environment terrorists operate in and the image of your organization. For instance, the Al Qaeda training manual states, “It is easier to attack a lamb than a lion.” Therefore, it is a basic assumption that terrorists will gradually find an easy target that will meet their needs, and develop an assault plan against that target. Terrorists choose a target that will achieve their goal, and then probe the target to determine if there is a vulnerability they can exploit. The vulnerability of your organization is directly related to the amount of time and effort you put into establishing and practicing an effective Homeland Defense Plan.

Responsible leaders act in an organized well-planned manner to potential events. A Homeland Defense Plan requires the same effort you put towards your budget, marketing, advertising or production plans. In other words, develop your Homeland Defense Plan with the same importance you developed your financial and business plans.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

HAZARDOUS MATERIALS SECURITY (*HAZMAT Security*)

The terrorists are using our own resources against us!

Al Qaeda did not purchase the planes involved to attack the World Trade Center and the Pentagon. North America is a highly technical and industrial society. Hazardous materials are in abundance and used in many manufacturing processes; they are stored onsite at many locations and transported daily on our roads. Each community, corporation and organization must determine what and where these hazardous materials are and then ensure there are safeguards in place to prevent their misuse, theft or malicious destruction. Terrorists do not need to covertly import weapons of mass destruction. They only need to gain access to storage or manufacturing facilities that contain these hazardous materials. They can also steal the hazardous material for use somewhere else. The Oklahoma City bombing used a homemade fertilizer bomb whose main component was Ammonium Nitrate. This Nitrate based fertilizer is used on farms across the United States and usually stored in unsecured locations in bulk.

After the Alfred P. Murrah (Oklahoma City) bombing some manufacturers of Nitrate based fertilizers have added, in some instances, very small "Tagents" to their products. By adding Tagents, which can only be seen under a microscope, officials can track Nitrate based fertilizers from manufacturing through to their use. However, after the explosion has already occurred, what is the preventative value of Tagents outside of lending aid to the post-mortem investigation?

Judge for yourself:

- a.) Have you established and implemented security measures to control your hazardous materials?
- b.) Have you established and implemented effective screening methods to control purchases of your hazardous materials?
- c.) Can you control who has access to your hazardous materials?
- d.) Do you know if you have hazardous materials?

We, too, must take new measures to protect our cities, our resources and people from the threat we face today, the threat of terrorism. That is why today we announce the Homeland Security Advisory System. The Homeland Security Advisory System is designed to measure and evaluate terrorist threats and communicate them to the public in a timely manner. It is a national framework; yet it is flexible to apply to threats made against a city, a state, a sector, or an industry. It provides a common vocabulary, so officials from all levels of government can communicate easily with one another and to the public. It provides clear, easy to understand factors which help measure threat.

Governor Tom Ridge, Speech before the Nation, March 12, 2002

Copyright © 2002 Bulwarkz Defensive Solutions and WMD Task Force.
All rights reserved

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

LIABILITY FOR ORGANIZATIONS TARGETED BY TERROR ATTACKS (A Legal Perspective)

Protection of employees and company assets is not the only reason to incorporate Homeland Defense Plan issues into your company's emergency plans. Employees and other third parties who are harmed in such an attack may sue companies that are targeted by a terrorist attack.

For example, an article in a New York Law Journal special feature identified a host of entities against which plaintiffs might file suits arising from the September 11 terrorist attacks, if they choose to forego their rights to recover from the September 11th Victim Compensation Fund of 2001:

[T]he possible defendants are American Airlines and United Airlines, and various companies and organizations that participated in security work for the hijacked flights, Argenbright, Globe Aviation Services, Huntleigh USA Corp., Massport, Port Authority of New York and New Jersey (which directed some twin towers' employees to return to their desks), New Jersey, Metropolitan Washington Airports Authority, and the U.S. government for the activities of Air Traffic Control¹.

Even though the author of this article noted that the Act that authorized this fund might make it risky to sue these defendants², at least one lawsuit has been filed to date against United Airlines. Furthermore, employers could be faced with workers compensation claims, or tort lawsuits arising out of terrorist acts that harm or kill employees³.

One New York law firm that analyzed this risk after September 11 has suggested that employers:

“[S]eriously consider retaining an experienced and well-regarded security firm to conduct an independent audit of its security procedures. That is in part because if an employer's building were the subject of a terrorist attack, *victims would likely claim that the employer should have been on notice of a potential threat due to the gravity of the potential consequences of a terrorist incident . . .* In any event, *retention and use of such an expert would prove valuable in the eventuality of a lawsuit in helping to establish that the employer acted in a reasonable manner to secure its property and protect the people thereon*⁴. (Emphasis added)

¹ Kreindler, “Pros and Cons of Victims Funds,” New York Law Journal November 28, 2001.

² Id.

³ Rothman and Herman, “Potential Employer Liability Arising Out of an Incidence of Terrorism,” Employer Update (Weil, Gotshal & Manges Winter 2001) (www.weil.com). This article cites Lewis v. Knappen Tibbetts Abbett Engineering, a New York case in which the court awarded workers compensation benefits for a New York employee killed by terrorists while working in Israel.

⁴ Id.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

The same law firm also recommended that as part of any such audit, employers develop “reasonable and practicable security and evacuation protocols and procedures⁵.”

Evidence that such practices may ultimately be part of workplace safety requirements has also come from the government. After the anthrax letter attacks following September 11, OSHA issued guidelines designed to help employers protect employees from anthrax-laden mail.

Cyber Liabilities

Even if your company is not the victim of a physical terrorist attack, an attack on the company's information assets and computer network can also create loss and liability. The 2000 CSI/FBI "Computer Crime and Security Survey" indicated that 85% of the 538 companies surveyed had suffered an intrusion or exploit, and 64% stated that the intrusion or exploit resulted in a loss. Of these companies, 35% were able to quantify the loss in dollar figures that totaled \$377 million, for an average loss of about \$2 million. Third parties have already begun to file suits against entities whose network assets were used by hackers to harm these third parties. New statutes such as the Gramm-Leach-Bliley Act and HIPAA require companies to protect information assets involving sensitive information, such as financial or health information.

INTERFACING WITH EMERGENCY RESPONSE PLANNERS

Deterring and responding to terrorism is a community effort, especially in urban environments. You may have the best security and Homeland Defense Plan on the planet, but if the skyscraper next you does not, you may become an indirect victim due to a higher profile target located in your neighborhood. No community, corporation or organization is an island when dealing with weapons of mass destruction. Plans must be coordinated with neighbors and the first responders – fire, police and emergency medical units. Ultimately, everyone falls under the jurisdiction of the local government authorities, incident commander or the fire or police chief. Your individual plan should address what is called the “Golden Hour” – the first hour after a catastrophic incident. This is when the most lives can be saved. Ask yourself; “How am I going to protect my personnel and facilities until rescue personnel arrive and safe evacuation is established?”

However, we should not expect a V-T day, a victory over terrorism day anytime soon. But that does not mean Americans are powerless against the threat. On the contrary, ladies and gentlemen, we are more powerful than the terrorists. We can fight them not just with conventional arms, but also with information, expertise and common sense; with freedom, openness and truth; with partnerships born from our cooperation. If we do, then like the men and women who fought Nazism and Fascism 60 years ago, our outcome will be equally certain: victory for America, and safety for Americans. *Governor Tom Ridge, Speech to the Nation, March 12, 2002*

⁵ Id.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

APPENDIX A: THE AUTHOR'S BIOGRAPHICAL INFORMATION



Bill Corbitt
President, Bulwarkz Defensive Solutions (www.bulwarkz.com)
E-mail: bcorbitt@bulwarkz.com

Bill Corbitt is a recognized information security expert with nearly a decade of experience in compliance and security oversight and integration of TCP/IP “wired” networks and 802.11b wireless networks (WLANs). Mr. Corbitt is best noted for his design improvements to “Yagi” style unidirectional 2.4GHz antenna configurations that lead the way for greater reception of WLAN communications from ‘off site’ locations.

Prior to Bulwarkz Defensive Solutions, Bill Corbitt held various technical executive positions. His last position was as the Director of Managed Services for Fiderus Inc. in which Mr. Corbitt was the first in the company to break projected quarterly revenue goals and lace together various and mutually beneficial strategic partnerships. Through his efforts, Mr. Corbitt was potentially the first to effectively negotiate a Security Franchising Agreement with an international Managed Services Provider.

Mr. Corbitt’s first position, after departing the military, was that of vice president of Technical Assessments and Loss Control for INSUREtrust. There he designed and implemented the industry's first insurability rating process for computer networks. This is a standard that allows businesses to obtain network-liability insurance (“hacker insurance”) to diversify their risk exposure. Responsible for the worldwide security compliance and loss-control activities for INSUREtrust and its clients, Mr. Corbitt authored baseline security standards for the network operations centers and led security assessment teams, sales, corporate and industrial espionage investigations and strategic revenue-generation initiatives. *{After over two years and over one hundred clients, none of those clients to date have filed a claim against their insurance for a security breach.}*

While in the military Mr. Corbitt held various positions, his final position was Chief, Officer in Charge of emergency notification and information protection for U.S. Air Force Material Command Assets, Kirtland Air Force Base, New Mexico. He directed security policies, procedures and oversight relating to all chemical, biological and nuclear weapons convention treaties and activities, including information-protection programs for local and wide area networks.

Prior to departing the Air Force, Mr. Corbitt was a special agent for the U.S. Air Force Office of Special Investigations (OSI), with over eight years of investigative experience. He primarily investigated and countered acts of subversion, terrorism, foreign intelligence and corporate-industrial espionage, and managed personnel and resources for highly secure and classified computer networks.

Mr. Corbitt was also senior security officer for the USAF’s highly secure wireless facility, the High Energy Microwave Laboratory (HEML) located in Albuquerque, New Mexico. He led security oversight and integration for numerous classified Department of Defense (DOD) wireless initiatives, wireless threat modeling, and wireless countermeasures to thwart malicious interception of information pertaining to highly classified weapon system activities. *In the aftermath of the 1995 terrorist bombing of the Alfred P. Murrah building in Oklahoma City, Oklahoma, Mr. Corbitt was awarded the prestigious Oklahoma Governor's Commendation for his dedicated service and assistance.*

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002



John Bucciarelli
President, WMD Task Force (www.wmdtaskforce.com)
E-mail: jbuccia@wmdtaskforce.com

John Bucciarelli is a recognized expert in the areas of terrorism, weapons of mass destruction and domestic preparedness. John retired from the United States Army in July 2001. During the last four years of his military service he served in a counter-terrorism unit specifically designed to respond to domestic acts of terrorism involving weapons of mass destruction (nuclear, biological, chemical and conventional munitions). In this capacity, he interfaced with the Federal Bureau of Investigation, Federal Emergency Management Agency, Department of Energy, Department of Health and Human Services, United States Secret Service, United States Joint Forces Command, United States Army Forces Command, Department of Defense Joint Staff, United States Army Staff, Joint Special Operations Task Force, state agencies, and local authorities on matters of terrorism, weapons of mass destruction and domestic preparedness.

Since 9/11/01, he has been a frequent guest on radio talk shows across the United States and Canada. He has also been a frequent guest on Fox News and is a member of the NBC30 War Room team. Through this exposure to the public, John observed a tremendous void in the information and training available to the general public. When people talk about domestic preparedness and Homeland Security they are primarily referring to federal, state and local government agencies and the first responder community – fire, police and emergency medical personnel. John formed the WMD Task Force to fill this void and to empower Americans with information, knowledge and the tools to deter terrorism and reduce vulnerabilities.

The WMD Task Force is a national organization of retired military and veterans with education, expertise and education in terrorism, weapons of mass destruction and domestic preparedness. The WMD Task Force provides high quality disaster response training and support to communities, corporations and groups seeking to reduce the vulnerability of their organization to terrorist activities through vigilance, deterrence, education, training and planning to protect employees, critical infrastructures and facilities.

John holds a B.A in economics and psychology from Washington and Jefferson College. He is also a recognized expert and published author on leadership.

Publications: **LEADERS ARE MADE! A Building Block Approach to Effective Leadership and ARE YOU A LEADER?**

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002



Daniel J. Langin
Corporate Legal Counsel, Bulwarkz Defensive Solutions
E-mail: dlangin@bulwarkz.com

Dan has 9 years of experience in Internet, information technology and information security law. He has focused on counseling emerging technology and e-Business companies about the legal risks they face, and counseling insurance companies about the claims and coverage aspects of technology risk.

Dan currently divides his time between positions as General Counsel for healthcare solutions provider GeoAccess, Inc., as Corporate Counsel for Bulwarkz Defensive Solutions, Inc. (an Atlanta-based infosec company), and his own law and consulting practice, both solo and with Seattle-based risk consultants TechRiskLaw.com. Past legal experience includes positions as General Counsel of infosec solutions provider INSUREtrust.com and as IT Law Manager for the technology insurance groups of USF&G and St. Paul Fire & Marine Insurance Companies. He began his work in Internet, technology and media law (and insurance) in 1993 as Claims Counsel for Media/Professional Insurance, where he handled several early Internet claims and traditional defamation and intellectual property claims.

Dan has actively spoken and participated in policy roundtables on technology law and policy issues in the U.S., Canada, Europe and Israel, such as the Aspen Institute's Internet Policy Project, the American Bar Association's TIPS section, PLUS, and the BESTS roundtable on electronic commerce in Europe. He is an editorial board member of the Cyberspace Lawyer, and has published articles for it and the Defense Counsel Journal, Intellectual Property Counselor, Practising Law Institute (First Annual Internet Law Institute), the American Bar Association, and many others. He has been quoted in publications including USA Today, CIO Magazine, Computerworld, Boardwatch and the Boston Business Journal.

Dan is a 1988 graduate of the University of Iowa College of Law (where he was an editor of the Iowa Law Review), and a 1984 graduate (Magna Cum Laude) of Creighton University in Omaha, Nebraska. He served as judicial clerk to Justice Linda K. Neuman of the Iowa Supreme Court from 1988 to 1989.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

APPENDIX B

March 11, 2002 Homeland Security Presidential Directive-3

Purpose

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

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

Homeland Security Advisory System

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

Low = Green;
Guarded = Blue;
Elevated = Yellow;
High = Orange;
Severe = Red.

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

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

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response. Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting and maintaining these plans.

Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures. They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations = Protective Measures.

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

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

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

- a.) To what degree is the threat information credible?
- b.) To what degree is the threat information corroborated?
- c.) To what degree is the threat specific and/or imminent?
- d.) How grave are the potential consequences of the threat?
- e.) Threat Conditions and Associated Protective Measures

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

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

- 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. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- 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.

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

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

- 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. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- 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. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- 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.
- Comment and Review Periods

Homeland Defense Planning

A WMD Task Force and Bulwarkz White Paper

March 31, 2002

The Attorney General, in consultation and coordination with the Assistant to the President for Homeland Security, shall, for 45 days from the date of this directive, seek the views of government officials at all levels and of public interest groups and the private sector on the proposed Homeland Security Advisory System. One hundred thirty-five days from the date of this directive the Attorney General, after consultation and coordination with the Assistant to the President for Homeland Security, and having considered the views received during the comment period, shall recommend to the President in writing proposed refinements to the Homeland Security Advisory System.

