Threat Advisory System Response

GUIDELINE

ASIS INTERNATIONAL
Advancing Security Worldwide™

ASIS INTERNATIONAL COMMISSION ON GUIDELINES

The Commission on Guidelines was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector secure its business and critical infrastructure, whether from natural disaster, accidents, or planned actions, such as terrorist attacks, vandalism, etc. ASIS had previously chosen not to promulgate guidelines and standards, but world events have brought to the forefront the need for a professional security organization to spearhead an initiative to create security advisory provisions. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhancing the professionalism of the industry.

Mission Statement

To advance the practice of security through the development of risk mitigation guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives

- Assemble and categorize a database of existing security-related guidelines
- Develop methodology for identifying new guideline development projects
- Involve/organize ASIS Councils to support guideline development
- Identify and develop methodology for development, documentation, and acceptance of guidelines
- Develop and sustain alliances with related organizations to benchmark, participate, and support ASIS guideline development
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions

- Establish guideline project
- Determine guidelines for development and assign scope
- Assign participating Council(s), where appropriate
- Approve membership on guideline committee
- Act as a governing body to manage and integrate guidelines from various Councils and security disciplines
- Review and monitor projects and guideline development
- Approve Final Draft Guideline and Final Guideline
- Select guidelines for submission to the Security Industry Standards Council and the American National Standards Institute (ANSI)

ASIS INTERNATIONAL
Advancing Security Worldwide™

THREAT ADVISORY SYSTEM RESPONSE GUIDELINE

Considerations and Potential Actions in Response to the Department of Homeland Security Advisory System

ASIS GDL TASR 09 2004

ISBN 1-887056-53-X

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ASIS INTERNATIONAL
Advancing Security Worldwide™

Threat Advisory System Response (TASR) Guideline

1.0 ACKNOWLEDGMENTS

ASIS International would like to express its foremost appreciation to the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, in conjunction with BITS, the Technology Group for The Financial Services Roundtable, and the Securities Industry Association (SIA) for their cooperation and use of material, which was significant to the development of the Threat Advisory System Response (TASR) Guideline.

Additional appreciation is expressed to the following entities and organizations whose threat response plans, documentation, and general assistance proved notably valuable during the reviews performed while developing the TASR Guideline.

- California Anti-Terrorism Information Center
- International Association of Assembly Managers (IAAM)
- Boeing International Security Office
- U.S. Department of Justice, Office for Domestic Preparedness
- American Red Cross
- United Space Alliance Security & Facilities Services
- Marriott North American Lodging Operations
- The University of Findlay Center for Terrorism Preparedness
- Frozen Food Express Industries, Inc.
- Texas Gas Association

2.0 TITLE

The title of this document is the Threat Advisory System Response (TASR) Guideline.

3.0 REVISION HISTORY

Baseline Document.

4.0 COMMISSION MEMBERS

Sean A. Ahrens, CPP, Schirmer Engineering
Norman D. Bates, Esq., Liability Consultants, Inc.
Regis W. Becker, CPP, PPG Industries
Jerry J. Brennan, Security Management Resources, Inc.
Chad Callaghan, CPP, Marriott International, Inc.
Pamela A. Collins, Ed.D., CFE, Eastern Kentucky University
Michael A. Crane, CPP, IPC International Corporation
Edward J. Flynn, CFE, Protiviti, Inc.
F. Mark Geraci, CPP, Bristol-Myers Squibb Co.
L. E. Mattice, Boston Scientific Corp.
Basil J. Steele, CPP, Sandia National Laboratories
Don W. Walker, CPP, Securitas Security Services USA, Inc.

5.0 COMMITTEE MEMBERS

Randy Atlas, Ph.D., AIA, CPP, Atlas Safety & Security Design, Inc.
Phill Banks, PE, CPP, The Banks Group
Lawrence K. Berenson, CPP, L-3 Communications, Inc.
Jerry J. Brennan, Security Management Resources, Inc.
Matt Brodbeck, GE Aircraft Engines
Roger Callahan, Bank of America
John C. Cholewa III, CPP, Sprint Corp.
Jonathan Cofer, BG (Ret), MZM, Inc.
Michael A. Crane, CPP, IPC International Corporation
Thomas E. Dougherty, The Boeing Company
Windom D. Fitzgerald, CPP, Fitzgerald Technology Group
Joseph R. Granger, CPP, United Space Alliance
Cheryl M. Jenkins, United Space Alliance
Greg Jodry, E & J Gallo Winery
Kathleen L. Kiernan, Ed.D., MZM Inc.
Glen Kitteringham, M.Sc., CPP, Brookfield Properties Corp.
Robert F. Lang, CPP, Georgia Institute of Technology
Armando Lara, Control Risks Group, LLC
Peggy Lipps, Bank of America
James P. Litchko, Litchko & Associates, Inc.
Richard E. Mainey, Marsh & McLennan Companies, Inc.
Judith G. Matheny, CPP, CFE, Lehman Brothers Corporate Security
Henry A. Nocella, CPP, Nocella Security Consultancy, LLC
Nickolas W. Proctor, Brown & Williamson
Steve Ramsay, Ramsay Risk & Security Consulting
Deed L. Vest, United Space Alliance
Lewis E. Wagner III, CPP, CISSP, Clarian Health Partners, Inc.

6.0 KEYWORDS

Threat Level, Emergency Response, Business Continuity, Personnel Protection, Physical Protection.

7.0 GUIDELINE DESIGNATION

This guideline is designated as ASIS GDL TASR 09 2004.

8.0 SCOPE

The Threat Advisory System Response (TASR) Guideline is applicable in private sector environments, which must evaluate and possibly respond to changes in the Department of Homeland Security (DHS)/Homeland Security Advisory System (HSAS) Threat Level Matrix. There is an understanding that threats move along a continuum of probability. Keeping that in mind, intervention with an appropriate level of security can serve to harden the target, reducing the risk of an impending event.

Historical: Although the United States has been able to respond successfully to national disasters, conventional wars, and other calamities for years, the nature of threats and risks underwent profound change on September 11, 2001. Thereafter, the challenge of homeland security became significantly more complex and difficult, requiring a comprehensive national strategy.

Following the September 11 terrorist attacks on New York and Washington, D.C. the President signed Presidential Directive-3, establishing the Homeland Security Advisory System (HSAS), as part of a series of initiatives geared at improving coordination and communication among the various levels of government and the American public in the fight against terrorism. The HSAS characterizes suitable levels of vigilance, preparedness, and readiness in a sequence of threat conditions. The actions relative to each threat level are cumulative and build upon those actions detailed for the previous threat level. A heightened threat level can be declared for the entire nation or a limited geographic area or industrial sector.

Subsequently, on February 28, 2003, the President issued Presidential Directive-5, which enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system. Together, the two Directives provide a strong basis for the private sector to actively support the public sector in the war on terrorism.

9.0 SUMMARY OF GUIDELINE

The TASR Guideline is designed as a tool to allow an organization to decide upon and provide a security architecture characterized by appropriate awareness, prevention, preparedness, and response to changes in threat conditions. The Guideline is structured at a high level, although specific considerations and responses are also addressed for consideration by individual organizations based on specific risk assessment and requirements, which are applicable across a broad range of the private sector.

Availability of updated risk analyses at the organizational level is strongly recommended. These would preferably be developed during low threat level conditions (Green (Low)/Blue (Guarded) Alert Levels under the DHS model). The information gained from this kind of analysis may be of significant benefit in understanding threats, critical assets, targeted assets, vulnerabilities, protection requirements, and response options/challenges for threat levels Yellow (Elevated), Orange (High), and Red (Severe).

10.0 PURPOSE

Private business and industry, as the principal provider of goods and services and the owner of approximately 85 percent of the national infrastructure, play a significant role in helping to mitigate the physical effects and economic costs of domestic incidents. Business and industry collaboration with government and other organizations has become essential for protecting and restoring the nation's critical infrastructure in the event of an incident. The public-private sector partnership is a crucial component of the national strategy and infrastructure for combating terrorism.

ASIS International has developed the TASR Guideline as an initiative to provide private business and industry a tool to prompt consideration of possible actions that could be implemented based upon elevated Alert Levels announced by DHS. The Guideline, in conjunction with the HSAS, is intended to be used as a recommended baseline to derive ultimate threat responses.

The overarching objective is to balance the need for a tool both applicable and understandable to a large portion of the private sector, while also providing sufficient detail to be of practical use to the organization.

11.0 TERMINOLOGY

Antivirus Software – Programs to detect and remove computer viruses.

Business Continuity Plan – An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing, and maintenance.

Canned Message – A message that has been developed to be used in the event of an emergency. Messages may be pre-recorded and taped for playing at a later time or exist in a policy/procedure for future reference.

Central Command Center – A designated location from which the deployment of contingency procedures and plans can be implemented.

Contingency Procedures/Plans – Contingency procedures are alternatives to normal procedures when an unusual but anticipated situation occurs. Contingency plans set forth organized, planned, and coordinated courses of action to be followed in case of an emergency event such as fire, explosion, or release of hazardous waste.

Crisis Management Team – A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communication/media relations, manufacturing, warehousing, and other business critical support functions.

Cyber Isolation – The removal of an individual's or entity's computer network from access to the Internet.

Cyber Security – Security used to protect an individual's or entity's computer network access from criminal activity.

Denial of Service/Distributed Denial of Service (DoS/DDoS) – Internet-based attacks aimed at sending thousands of network packets to an organization's routers and servers for the express purpose of either shutting down those devices or preventing the flow of normal business traffic.

Duress Alarm – A device that enables a person placed under duress to call for help without arousing suspicion.

EMS – Emergency Medical Service.

Emergency Response Team – The private sector response team at the scene to resolve the critical incident.

Expatriate Employee – Person engaged in services for wages or salary by an organization and physically located in a country that is not his/her native country.

Externally Facing Websites – Websites that permit access to an organization's website from locations outside of the organization.

Firewall – A combination of hardware and software that filters computer network traffic from and to the Internet based upon network access control parameters. A firewall can mask internal network information as well as stop exploratory probes and denial of service attacks.

First Responders – A generic term to describe the members of an organization's medical Emergency Response Team or those individuals, such as fire, police, emergency medical service providers, and other law enforcement personnel, whose duty is to be the first people at the scene of a critical incident.

HVAC System – Heating, ventilating, and air-conditioning system.

Information Security Risk Management Program – The overall strategic and tactical roadmap used to assess threats, their impacts to critical information and resources, prioritization of those impacts, recommended countermeasures to mitigate those impacts, and continual management of the security process.

Integrity Seals – A seal that provides clear evidence that it has been tampered with or illegitimately opened and whose forcible removal would result in the visible destruction of its essential parts.

IT Intrusion Detection System – Hardware and software designed to monitor critical network and host server (i.e., computer) traffic and transactions for the express purpose of alerting security and technical administrators of suspicious and/or unauthorized activity.

Look-Back (Inwards) Surveillance – A method of surveillance that concentrates on reviewing and evaluating individuals and equipment that is focused on monitoring one's activities.

Manual Evacuation – The physical removal of people and property by hand to another, more secure location.

MOA – Memorandum of Agreement.

MOU – Memorandum of Understanding.

PBX – Private Branch Exchange. The telephone network used by an organization to allow a single access number to offer multiple lines to outside callers and to allow internal staff to share a range of external lines.

Shelter in Place – The process of securing and protecting people and assets in the general area in which a crisis incident occurs.

Staging – The assembling of material, equipment, etc. in a particular place.

Tabletop Exercise – A test method that presents a limited simulation of an emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.

12.0 HOW TO USE THE TASR GUIDELINE

The TASR Guideline primarily addresses security concerns and considerations in response to the Department of Homeland Security's Advisory System. No guideline can anticipate all eventualities that result from acts of terrorism or provide specific direction with respect to individual situations. This Guideline has been prepared for the sole purpose of assisting the reader to prepare plans, procedures, and response strategies that may contribute to the mitigation of potential threats and risks.

Organizations vary with respect to the level of security that is a part of their normal operations. Some may operate in an unrestricted environment, while others maintain a level of rigorous security and access control 24/7. Once it is understood where an organization's operations fall within the Green/Blue Advisory Level, the TASR Guideline can be tailored to fit the needs of the organization.[1] Each suggested response should be used only as a possible consideration, which can be modified according to specific needs and circumstances.

It is strongly recommended that users of the TASR Guideline first conduct a security risk assessment of their facilities, electronic information infrastructure, assets, and personnel, utilizing one of the many models that exist as a guide. ASIS International publishes the General Security Risk Assessment Guideline (http://www.asisonline.org/guidelines/guidelines.pdf). ASIS' General Security Risk Assessment Guideline is a seven-step process that creates a methodology by which security risks at a specific location can be identified and communicated, along with appropriate solutions. Ideally, this should be done in either the Green/Low or the Blue/Guarded Advisory Level as a routine business practice, thus affording preparation for responding to heightened HSAS threat levels.

It is suggested that activities at previous lower levels be continued in addition to those at elevated levels. To avoid redundancies, these suggested activities are not repeated in the matrices at higher threat levels. Availability of updated risk analyses, as recommended for preparation during Green/Blue Threat conditions, may be of significant benefit in understanding threats, critical assets, targeted assets, vulnerabilities, and response options/challenges for levels Yellow, Orange, and Red.

References are made to evaluations of detailed systems within the organization such as IT, HVAC, security access control/intrusion detection systems, etc. The reader is encouraged to contact his/her manager/security provider/consultant for more specific expertise related to such systems.

Structure of THREAT RESPONSE MATRIX: The TASR Guideline Matrix is divided into four major sections—Green/Blue, Yellow, Orange, and Red—and further broken out by three subcategories as follows:

Category 1: Emergency Response—Business Continuity

[1]The Homeland Security Advisory System designates Green and Blue as two distinct levels. For ease of understanding and implementation of the ASIS Threat Advisory System Response Guideline, the Green and Blue levels have been combined into one.

Category 2: Personnel Protection

Category 3: Physical Protection

Please Note: For ease of understanding, steps outlined under ''Considerations & Potential Actions'' are additive. Each succeeding level incorporates all activities from the previous levels.

To use the matrix:

1. Identify the impending threat.[2]
2. Identify the National Threat Advisory Level released by the Department of Homeland Security and review actions identified with the corresponding advisory level.
3. Determine if the imposing threat can be considered against a critical infrastructure and/or at what level (National/Regional/State/Local) the threat applies.
4. Determine applicability of considerations and potential actions to personnel, assets, and facility(s).
5. Determine response to be taken.

[2]The Homeland Security Advisory System designates Green and Blue as two distinct levels. For ease of understanding and implementation of the ASIS Threat Advisory System Response Guideline, the Green and Blue levels have been combined into one.

13.0 THREAT LEVEL MATRIX
(Developed from the Homeland Security Advisory System)

THREAT LEVEL	NATIONAL (Including Critical Infrastructure)	REGIONAL/STATE/LOCAL
RED or SEVERE R	Declared when there is a severe risk of a terrorist attack or when an incident occurs or credible intelligence information is received by a critical infrastructure that a terrorist act is imminent.	Declared when a terrorist attack has occurred or credible intelligence indicates that one is imminent, that has prevention and response characteristics of a regional/state/local nature and that a specific target has been identified.
ORANGE or HIGH O	Declared when there is a high risk of a terrorist attack or when a credible threat exists of terrorist activity against one of the critical infrastructures.	Declared when credible intelligence indicates that there is a high risk of a terrorist attack having prevention and response characteristics of a regional/state/local nature, but a specific target has not been identified.
YELLOW or ELEVATED Y	Declared when there is a significant risk of a terrorist attack or when a general threat exists of terrorist activity against one of the critical infrastructures.	Declared when there is an elevated risk of terrorist attack, but a specific region of the U.S. or target has not been identified.
BLUE or GUARDED B*	Declared when there is a general risk of terrorist attacks or when there is a general risk of terrorist attacks against one of the critical infrastructures.	Declared when there is a general risk of terrorist attacks.
GREEN or LOW G*	Declared when there is a low risk of terrorist attacks against one of the critical infrastructures.	Declared when there is a low risk of terrorist attacks.

* The Homeland Security Advisory System designates Green and Blue as two distinct levels. For ease of understanding and implementation of the ASIS Threat Advisory System Response Guideline, the Green and Blue levels have been combined into one.

14.0 RECOMMENDED PRACTICE ADVISORY: THREAT RESPONSE MATRIX

Level 1 Green/Blue Threat Levels					
Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
Emergency Response—Business Continuity					
1	G	B	Develop/enhance organization Business Continuity Plan. (An organization should develop a business continuity plan that will address such topics as readiness, prevention, response, recovery/resumption, testing and training, and evaluation and maintenance.)		
2	G	B	Establish Crisis Management Team and other related Response Teams, such as an Emergency Response Team, Incident Response Team, Disaster Recovery Team, etc. and train as to their responsibilities relative to each threat level.		
3	G	B	Prepare to implement aspect of the Business Continuity Plan and contingency plan within the context of the current threat.		
4	G	B	Review and validate procedures for heightened alert status.		
5	G	B	Establish a central command (crisis management) center from which to direct contingency plans, response, and recovery/ resumption operations. Ensure appropriate communications equipment is installed and functioning including radios, cell phones, and Internet access.		
6	G	B	Prepare for the possibility of flooding or other destruction as a result of a bombing incident or other similar catastrophic events.		
7	G	B	Establish a prioritized roster of people to direct emergency response procedures.		
8	G	B	Review processes to support personnel who may be called to active military duty. Address return to work, benefits, leave procedures, etc.		
9	G	B	If possible, track locations of expatriate personnel on assignment and vacation in foreign countries and review contingency procedures for possible evacuation.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
10	G	B	Review budgets to support required security measures as costs increase due to a heightened threat level. Determine if partnerships can be leveraged with other organizations to reduce costs.		
11	G	B	Develop tabletop exercises of procedures that may be appropriate.		
12	G	B	Plan for an alternate work site in the event of an evacuation, including the staging of non-perishable food, sleeping bags, medical supplies, water, miscellaneous supplies, etc. for key personnel needed to occupy the location. Be prepared to replicate critical company paper and electronic records (financial, personnel, legal, etc.), communications, and IT processing capabilities at relocation facility.		
13	G	B	Provide for the safekeeping of critical company records, i.e., financial, personnel, legal, etc.		
14	G	B	Perform emergency evacuation drills with all building staff to simulate actual conditions and practice response procedures.		
15	G	B	Develop rapport and maintain a liaison with local law enforcement, fire, and medical responders and develop communication methods and alternatives. Provide names and phone numbers for key contact personnel to the emergency response organizations. Insure local agencies' familiarity with the physical layout and operational procedures. Designate arrival location for emergency response vehicles.		
16	G	B	Consult with local first responders and other government agencies regarding best actions to develop relative to ''shelter in place.''		
17	G	B	Invite local fire, police, EMS, and regulatory agencies in training exercises designed for the organization's Crisis Management Team and related Response Team(s).		
18	G	B	Work with local EMS first responders to establish pre-designated triage locations and backups.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
19	G	B	Develop a media relations and communications strategy, including a selected staging area for the media. In addition, provide additional media training for designated personnel.		
20	G	B	Make arrangements for mental health counselors for personnel should a devastating event occur.		
21	G	B	Establish a crisis hotline to take calls from and to provide information to personnel, family members, and others affected by an incident.		
22	G	B	If an organization has medical personnel associated with operations, verify response plans are current.		
23	G	B	Ensure that the organization's first responders are certified in First Aid, Cardiopulmonary Resuscitation (CPR), and the use of Automatic External Defibrillators (AEDs).		
24	G	B	Develop relationships and documents (MOUs, MOAs), if appropriate, with state and federal agencies, including emergency management, law enforcement, and the military. Determine if partnerships can be leveraged with other organizations to reduce costs.		
25	G	B	Contact vendors and suppliers critical to the operation and confirm their emergency response plans.		
26	G	B	Establish a process for periodic monitoring of TV, radio, and news reports and incorporating this capability in the central command center.		
27	G	B	Develop canned messages (approved by organization's leadership) that can be disseminated to the workforce at the announcement of various alert levels. Determine when, by whom, and how those messages will be disseminated.		
28	G	B	Plan for alternate means of communications if phone lines are not available. Determine availability of satellite capability to support communications, if cell phone reception is not available.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
29	G	B	Maintain independent emergency lines separate from facility PBX. In addition, develop back up/ alternate methods of communications.		
30	G	B	Determine the threats to existing/proposed information technologies. Establish an information/data security risk management program.		
31	G	B	Review and validate information/data security response plan, if established.		
32	G	B	Create an information technology security education and awareness program for technical administrators, key focal points, and the organization's general population.		
33	G	B	Establish comprehensive employee training program addressing information/data security.		
34	G	B	Refresh employees' knowledge of social engineering techniques designed to trick employees into divulging information that could be used to compromise data security.		
35	G	B	Review information posted to web sites and be prepared to remove it if the information compromises security.		
36	G	B	Coordinate appropriate information technology security measures and programs with all key corporate, local, state, and federal security entities to ensure enhanced protection and response.		
37	G	B	Plan for and pre-position critical supplies of network, system, and other information technology hardware, firmware, and software so that during emergencies adequate levels of network and system access are not interrupted due to loss of any one component.		
			Personnel Protection		
38	G	B	Provide key personnel, vendors, suppliers, and contractors a copy of the facility emergency procedures and other pertinent organizational guidelines.		
39	G	B	Develop training for employees, including alternate site employees, covering high risk/ critical functions, especially when functions are not conducted on a routine or daily basis.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
40	G	B	Develop emergency procedures and training for people with special needs.		
41	G	B	Train all personnel to raise their minimal level of security awareness to their surroundings and activities that may occur and the development of family plans. Determine training and guidelines for shelter in place plans and rationale.		
42	G	B	Determine placement/location of Automatic External Defibrillators (AEDs) to support timely response to emergencies. Require the development of AED protocols and training of Crisis Management Team and related Response Team(s) members.		
43	G	B	If established, validate that existing security access control/intrusion detection systems, i.e., cameras, alarms, locks, lighting, card access devices, etc., are in good working order. Have serviced, if needed.		
44	G	B	Establish a neighborhood watch program with surrounding communities.		
45	G	B	Establish a program to track employees' business travel and remote assignment locations.		
46	G	B	Encourage employees to volunteer at emergency organizations.		
47	G	B	Review and validate that basic training of response personnel is current and adequate in context of possible threat condition to the organization.		
48	G	B	Be cognizant of current events. Monitor TV, radio, and newspaper reports.		
49	G	B	Prepare contingency plans for loss of water, heat, air conditioning, and electrical power.		
Physical Protection					
50	G	B	Review and verify availability of additional/back-up personnel to support security and facilities functions.		
51	G	B	Develop look-back and inwards surveillance plans (''watch who is watching you'').		
52	G	B	Prepare and review risk assessments performed against facilities, assets, and personnel.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
53	G	B	Encourage the community to report suspicious activities, i.e., photographing the facility or government buildings, bridges, dams, water systems, power systems, interstate highway nodes, or asking detailed questions about security at these critical facilities.		
54	G	B	Train security personnel on acceptable and appropriate responses to civil disturbances, demonstrations, protests, etc.		
55	G	B	Make facility master keys available to appropriate personnel.		
56	G	B	Perform background checks on all full-time service contractor employees.		
57	G	B	Perform penetration tests of access control and intrusion detection systems.		
58	G	B	Install cameras for surveillance on equipment outside or adjacent to facilities, if not already in place.		
59	G	B	Develop procedures to perform inspections of items carried into the facility by personnel, contractors, and visitors.		
60	G	B	Develop plans and consider utilizing identified and unidentified security vehicles.		
61	G	B	Train security guards on special requirements unique to organization, e.g., vehicle inspection techniques.		
62	G	B	Install (or verify operation of) duress alarms from the receptionist desk and/or remote guard stations, executive offices, and key access points to the central command center.		
63	G	B	Equip receptionist phone with a notification to the central command center indicating a telephone off-hook situation.		
64	G	B	Develop plans for restricting vehicle access.		
65	G	B	As appropriate, install barricades, i.e., large flowerpots, cement stanchions, etc. to prevent vehicles from driving through facility entrance doors/gates.		

Threat Level			Considerations & Potential Actions	Applies Y/N	Response Notes
66	G	B	Know how to turn off power, gas, and water. Ensure procedures are ready for dealing with emergency shutdowns of HVAC systems in the event of a possible internal or external chemical release.		
67	G	B	Designate a ''safe'' interior location, which has a self-contained HVAC and filter system for personnel, in the event HVAC systems are shut down.		
68	G	B	Identify backup power sources and verify that they are operational. Ensure long-term availability of diesel fuel for emergency power generation through contractual obligations with suppliers, if appropriate. Further, determine priority of sequence of availability with other organizations, including government, as others may have precedence.		
69	G	B	Obtain and/or review facility maps, plans, as-built drawings, etc. for accuracy and secure in safe place for referencing.		
70	G	B	Determine secured storage alternatives if hazardous or other critical materials are present in or around facilities.		
71	G	B	Install emergency buzzers from dock ingress and egress to central command center.		
72	G	B	Designate limited locations for receipt of mail.		
73	G	B	Establish plans for an alternate emergency operations center at the organization's relocation facility from which to direct response and recovery operations if the primary facility is evacuated. Ensure appropriate communications equipment is installed and will be functioning including radios, cell phones, and Internet access.		
74	G	B	Ensure emergency exits are not obstructed and are clear of debris. Conduct periodic patrols to ensure compliance.		
75	G	B	Survey surrounding areas to determine those activities that might increase security risks, e.g., airports, government buildings, industrial facilities, pipelines, etc.		

Level 2 Yellow Threat Level				
Threat Level		**Considerations & Potential Actions**	**Applies Y/N**	**Response Notes**
Emergency Response—Business Continuity				
1	Y	Ensure all business, emergency, and continuity/ recovery plan documents are up to date, e.g., contact lists, notification/escalation procedures. Review and validate internal emergency communication plans for accuracy of names and numbers.		
2	Y	Conduct tabletop exercises of procedures that may be appropriate.		
3	Y	Convene Crisis Management Team and other related Response Teams to review emergency response and business continuity/recovery plans. Confirm functional responsibilities.		
4	Y	Review and refine emergency response processes within the context of the current threat information.		
5	Y	Verify cell phones and pagers are ready for distribution to the members of the Crisis Management Team and related Response Teams. Determine if cell phones should have text messaging capability.		
6	Y	If established, verify equipment, communications lists, and processes in the central command center.		
7	Y	Verify contacts and communicate with the law enforcement community and local outside emergency/medical, fire, and response personnel.		
8	Y	Obtain threat and intelligence updates from local, state, and federal authorities as well as private industry security sources.		
9	Y	Review the list of individuals notified by automatic alerts generated by security monitoring systems, e.g., network and IT intrusion detection systems, etc.		
10	Y	Reinforce user awareness in context of organizational requirements.		
11	Y	Review recovery plans to ensure they represent current situations/environments.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
12	Y	Implement procedures/software to stop potentially hostile/suspicious attachments at the email server. Create tighter levels of firewall, antivirus, and IDS filters so that they can readily be implemented in the event of an attack.		
13	Y	Review use of IT security filtering which may include upgrading firewalls and anti-virus software to ensure effectiveness of precluding electronic penetration of organizational systems.		
14	Y	Update checklists, focal points, and information technology inventories.		
15	Y	Perform penetration testing of individual organizational sites and encourage participation by vendors to validate cyber-security levels.		
		Personnel Protection		
16	Y	Implement employee training, including training of alternate site employees covering high-risk/critical functions, especially when functions are not conducted on a routine or daily basis.		
17	Y	Emphasize and elevate the importance of knowing planned absences, arrivals, and whereabouts of all personnel.		
18	Y	Be prepared to address sensitive issues relative to personnel expressing opinions either for or against threat prevention.		
19	Y	Ensure security-related information is communicated to personnel across the organization as approved by leadership.		
		Physical Protection		
20	Y	Ensure communication channels and processes are open, reliable, and consistent. Ensure alternative/ back up forms of communications are available.		
21	Y	Periodically review actions taken to date against the stated threat conditions as they may rapidly change for either better or worse.		
22	Y	Perform inspections of items carried into the facility by employees, contractors, visitors, etc.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
23	Y	Implement any special security programs supported by trained personnel.		
24	Y	Review and verify vehicle inspection training for security personnel.		
25	Y	Maintain a high index of suspicion and remain alert to unusual activities, occurrences, and behavior.		
26	Y	Refresh employees' knowledge of the danger of malicious code delivered by email via worm, viruses, etc.		
27	Y	Provide daily summary to key management and security personnel.		
28	Y	Ensure security checks with other integrated security consoles.		
29	Y	Monitor news media and emergency and law enforcement bulletins.		
30	Y	Lock down access points after normal business hours and restrict access as appropriate.		
31	Y	Perform housekeeping of exterior grounds of facilities limiting the storage of items, i.e., crates and other objects, that would otherwise provide camouflage.		
32	Y	Enhance or provide manned coverage of dock areas, if not already doing so.		
33	Y	Verify truck driver's license, bill of lading, and other applicable paperwork relative to deliveries.		
34	Y	Physically inspect cargo as necessary.		
35	Y	Consider increasing screening activity of inbound packages.		
36	Y	File travel itineraries of all Crisis Management Team members and related Response Team members with appropriate management.		
37	Y	Review and file travel itineraries of high-level executives with security director or equivalent to evaluate risk and safety.		
38	Y	Validate all building alarms, access controls, intrusion detection systems and building systems in accordance with threat conditions.		
39	Y	Evaluate off-site equipment storage.		

Level 3 Orange Threat Level				
Threat Level		**Considerations & Potential Actions**	**Applies Y/N**	**Response Notes**
Emergency Response—Business Continuity				
1	O	Implement emergency and contingency plans as necessary.		
2	O	Increase frequency of threat intelligence updates.		
3	O	Restrict staff travel and vacation for Emergency Response/Crisis Management Team(s).		
4	O	Convene Emergency Response/Crisis Management Team(s) to review the more specific information that is available from law enforcement, the media, and other sources to access the potential impact to the organization.		
5	O	Provide cell phones and pagers to the members of the Crisis Management Team and related Response Teams, if not already done.		
6	O	Verify alternate locations are valid and personnel supporting recovery operations are current in their obligations.		
7	O	Verify supplies are staged, secured, and complete to support recovery operations.		
8	O	Evaluate externally facing websites and, where necessary, close down non-essential services. For remaining sites, ensure all operating systems and related application software patches are applied. Ensure organizational security specialists have reviewed the organization's security definition for currency.		
9	O	Enhance monitoring of activity on essential services for externally facing websites to identify deviations from normal activity.		
10	O	Enhance monitoring of logging and intrusion detection for remaining sites, and review reporting mechanisms that are linked to an intrusion alert/ notification system.		
11	O	Validate distributed-denial-of-service preparedness (Check with Internet service provider for capability to assist, e.g., block address ranges, etc.)		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
12	O	Increase alert status for IT security personnel consistent with the organization's Business Continuity Plan.		
13	O	Prepare for ''cyber-isolation'' of non-essential individuals' outside connections.		
		Personnel Protection		
14	O	Be prepared to address issues related to personnel who serve in the military and may be called to serve.		
15	O	Be prepared to support personnel whose family members have been called to serve.		
16	O	Instruct personnel to report immediately suspicious activity, packages/articles, people, and vehicles to security personnel. Be cognizant of unattended packages/articles and vehicles.		
17	O	Instruct personnel to direct all press inquiries to the organization's Public Affairs office or equivalent.		
18	O	Review and validate that alternate travel arrangements are plausible in case modes of transportation are not available.		
19	O	Discuss risks associated with travel to foreign countries with the security director or equivalent.		
20	O	Cease travel to cities against which specific threats have been made.		
		Physical Protection		
21	O	Review plans to address any redirection or constraint to transportation systems. Consult with local authorities about control of public roads and accesses that might make the facility more vulnerable if they were to remain open.		
22	O	Discuss and coordinate with facilities and building management other security controls for guests and vendors.		
23	O	Prepare for possible evacuation, closing, and securing of all individual organization facilities.		
24	O	Increase security patrols internally and externally. Determine increased officer requirements for extended periods. Possibly suspend holidays, etc. and hold discussions with contract security providers for increased human resources.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
25	O	Assign additional staff in the central command center to monitor existing security cameras in real time.		
26	O	Evaluate the use of special foot patrols, bicycle patrol, etc. Use canine patrols if appropriate (campus environments).		
27	O	Increase surveillance of all facilities and take increased precautions.		
28	O	Evaluate requiring special identification for day labor, i.e., special badges, colored wristbands, etc. Inspect government issued photo ID as proof of identification each time. Special access identification should be provided each time for entrance to the facility and retrieved upon departure.		
29	O	Evaluate vehicle inspection program to include checking beneath the undercarriage of vehicles, under the hood, and in the trunk.		
30	O	Approach all illegally parked vehicles in and around facilities. Question drivers and direct them to move immediately. If owner cannot be identified, have the vehicle towed.		
31	O	Implement random shift changes of security guards.		
32	O	Coordinate with facilities and building management and increase inspections in and around the facility to ensure utility and emergency systems are not tampered with, damaged, or sabotaged. This includes emergency generation and lighting, fire alarms, and perimeter protection.		
33	O	Evaluate arranging for security or law enforcement vehicles to be parked randomly near access points and exits.		
34	O	Prepare to restrict access to essential personnel only.		
35	O	Limit driveway and parking area access as appropriate.		
36	O	If feasible, discontinue, limit, or otherwise control inside perimeter parking. Evaluate eliminating underground parking at this threat level.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
37	O	Increase inspections on building systems and infrastructure, including HVAC systems. Review ability of facilities and building management to rapidly shut down HVAC equipment. Discuss conditions whereby HVAC is to be shut down and also restarted.		
38	O	Inspect and, if feasible, secure vacant rooms (e.g., meeting, guest, housekeeping, storage, etc.)		
39	O	If permissible, in compliance with fire code, restrict access to rooftops or, at a minimum, monitor with response.		
40	O	Evaluate restricting services provided by outside vendors/suppliers (e.g., cleaning crews, etc.) to possible non-sensitive areas.		
41	O	Coordinate security in non-organization owned locations to coordinate effective security enhancements.		
42	O	Enhance visibility in and around perimeters by increasing lighting and removing or trimming vegetation.		
43	O	If elevators are on premises, train staff in operation of the elevator and the correct response in the event of an emergency.		
44	O	Validate vendor lists for all routine deliveries and repair services.		
45	O	If conditions warrant, conduct heightened screening of all inbound mail. Direct attention to any packages or letters received without a return address or having indications of stains/powder.		
46	O	Visually and physically inspect all expected and unexpected deliveries.		
47	O	Coordinate operations relative to critical infrastructure concerns with armed forces, i.e., armed security, local law enforcement, or the military.		
48	O	Discontinue tours and cease other non-essential site visits.		
49	O	Staff central command center, if in existence, during normal operational hours and continue to review call lists for currency. Run call tests and verify all equipment operational.		

Level 4 Red Threat Level				
Threat Level		**Considerations & Potential Actions**	**Applies Y/N**	**Response Notes**
Emergency Response—Business Continuity				
1	R	Convene Crisis Management Team and related Response Teams to manage and direct emergency response and/or business continuity/recovery plans in response to an imminent threat or actual event that impacts the organization, its employees, or third party vendors/suppliers, etc.		
2	R	Operate the central command center, if in existence, full staff 24/7.		
3	R	Notify law enforcement of facility evacuation and closings.		
4	R	Prepare to close the facility, protect assets, and shut down equipment and systems in the event of evacuation. Determine ahead of time who, if anyone, will remain behind to protect and monitor facility. Determine how and when facility will be re-opened.		
5	R	Extract and maintain a pre-determined number of communication lines (telephone, fax, and Internet) for emergency purposes.		
6	R	Prepare to evacuate personnel and items needed to support recovery operations.		
7	R	Prepare for ''manual evacuation'' of essential computer hardware and systems, including support requirements necessary to an alternate location of operations.		
8	R	Restrict access to facilities, equipment, systems, and essential personnel only.		
Personnel Protection				
9	R	Recommend personnel vary routes driven to work.		
10	R	Furlough non-essential personnel, institute flexible leave policy, or employee dispersal.		
11	R	Remind employees to direct all press inquiries to the Public Affairs department or equivalent.		
12	R	Eliminate travel into an area affected by a terrorist attack or an area that is a target of an attack.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
13	R	Cancel attendance at non-critical or off-site meetings, conventions, symposia, etc.		
14	R	Reinforce security awareness of surroundings at all times to avoid being a victim of a terrorist attack or a crime.		
15	R	Check emergency supplies, restock if necessary, and place in a handy place.		
16	R	Keep fuel tanks in vehicles full.		
17	R	Avoid passing on unsubstantiated information.		
18	R	Make available mental health counselors for employees as required and activate crisis hotline where appropriate.		
Physical Protection				
19	R	Cancel or postpone any individual organization-sponsored or hosted events.		
20	R	Pre-position specially trained teams or emergency response personnel.		
21	R	Implement plans to accommodate redirection or constraint of transportation.		
22	R	Redirect personnel to address critical emergency needs.		
23	R	Increase the number of security guards, guard postings, and roving guard visibility.		
24	R	Utilize alternate, enhanced methods of inspection at designated access points.		
25	R	Enhance monitoring of all buildings and access control/intrusion detection systems, i.e., cameras, alarms, locks, lighting, card access devices, etc. Ensure frequent checks with other integrated security consoles.		
26	R	Prepare to assist with evacuation and other emergency processes. Work in a coordinated effort with organizational security personnel and law enforcement as directed.		
27	R	Limit access points to minimal portals necessary to conduct operations.		

Threat Level		Considerations & Potential Actions	Applies Y/N	Response Notes
28	R	Inspect vacant buildings/rooms and use integrity seals, where possible, or lock down non-essential areas.		
29	R	Prepare to close facilities and shut down equipment in the event of evacuation and coordinate with security personnel. If warranted, disconnect organization's networks from the Internet.		
30	R	Confirm status and availability of any off-site equipment storage.		
31	R	Cancel or delay all non-vital facility work conducted by contractors, or continuously monitor their work with company personnel as applicable.		

15.0 REFERENCES/BIBLIOGRAPHY

REFERENCES

American Gas Association, Interstate Natural Gas Association of America, American Public Gas Association. *Security Measures.* Garland, TX: Texas Gas Association, 2002.

American Red Cross. *Homeland Security Advisory System Recommendations.* Washington, DC: American Red Cross, 2002.

ASIS International. *ASIS Disaster Preparation Guide.* Alexandria, VA: ASIS International, 2003.

California Anti-Terrorism Information Center. *California Anti-Terrorism Information Center Situational Unit.* Sacramento, CA: California Anti-Terrorism Information Center, 2002.

Corporate Security & Safety Advisory Board and the Law Enforcement Advisory Board for the University of Findlay, Center For Terrorism Preparedness. *Principles & Protocols of Threat Assessment Management "A White Paper."* Findlay, OH: The University of Findlay, Center For Terrorism Preparedness, 2002.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. Proprietary and Confidential working draft (March 2003), *Actions Relevant To The Homeland Security Advisory System.*

Frozen Food Express Industries, Inc. *Anti-Terrorist Action Plan.* Dallas, TX: Frozen Food Express Industries Inc., 2002.

International Association of Assembly Managers Safety and Security Task Force, *Best Practices Planning Guide for Convention Centers and Exhibit Halls.* Irving, TX: Center for Venue Management Studies, International Association of Assembly Managers, 2002.

U.S. Department of Justice. Office for Domestic Preparedness. *Emergency Responder Guidelines.* Washington, DC, 2002.

U.S. Environmental Protection Agency Water Protection Task Force. *Threat Advisory – Amended to Comport with WDNR General Security Recommendations.* Washington, DC, 2003.

BIBLIOGRAPHY

American Institute of Architects (AIA). *Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients.* Washington, DC: American Institute of Architects, 2001.

American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE). Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents on *Risk Management Guidelines for Health, Safety and Environmental Security under Extraordinary Incidents.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., 2003.

Atlas, Randall I. *Crime Prevention Through Environmental Design,* Chapter 19, part VIII in Protection of Assets Manual. Los Angeles, CA: POA Publishing LLC, 2000.

Demkin, Joseph A., ed., *Security in the Built Environment: A Planning and Design Guide for Architects and Design Professionals*. Washington, DC: American Institute of Architects, 2002.

European Committee For Standardization, Technical Committee CEN/TC 325. European Pre-standard. *Prevention of Crime – Urban Planning and Design – Part 2: Urban Planning*. Final Draft prENV 14383-2 (May 2002). Brussels: European Committee For Standardization.

Federal Emergency Management Agency (FEMA). *State and Local Mitigation Planning How-to Guide: Integrating Human-Caused Hazards into Mitigation Planning*. Washington, DC: Federal Emergency Management Agency, 2002.

Maher, Mary *"Serious About Security: Paying Attention to What We Protect and How,"* University of Wisconsin-Madison Department of Engineering Professional Development, 2002. http://aec.engr.wisc.edu/resources/rsrc17.html

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 33,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine — *Security Management* — ASIS leads the way for advanced and improved security performance.

Advancing Security Worldwide™

1625 Prince Street
Alexandria, VA 22314-2818 USA
703-519-6200
Fax: 703-519-6299
www.asisonline.org