McMANIS & MONSALVE ASSOCIATES

Threat, Risk and Vulnerability Assessment

Statement of Qualifications and Services

July 2011

Prepared by:
Marco Monsalve
McManis & Monsalve Associates
100 State Street, Suite 103
Erie, PA 16507
Phone: 814-454-4000
mmonsalve@mcmanis-monsalve.com

TABLE OF CONTENTS

CORPORATE PROFILE 1

EXPERTISE 2

SERVICES 3

THREAT, RISK AND VULNERABILITY ASSESSMENTS 3

EXAMPLES OF OUR WORK 5

Walter Reed Army Medical Center 5

The National Institutes of Health (NIH) 6

NAID Bioterrorism Research RBL and NBL Grantees 7

Perimeter Security for the Nuclear Regulatory Commission's Headquarters Facility .. 7

City of Hamilton, Montana, Vulnerability & Risk Assessment of Water and Wastewater Facilities 7

Department of Homeland Security, Office of Infrastructure Protection, and Office of Cybersecurity and Communications, Critical Infrastructure Warning Information Network Need and Mission Risk & Threat Assessment Study 7

Capitol Trailways Antiterrorism Security Assessment 8

CORPORATE PROFILE

McManis & Monsalve Associates (McManis & Monsalve) is a leading management consulting firm dedicated to helping government, corporate, and industrial enterprises protect their assets, ensure organizational continuity, service delivery, and profits. We clearly understand that security represents a significant expense which – if improperly executed – hinders productivity, efficiency, profitability, and successful asset protection.

Our extensive and successful management consulting experience is an excellent foundation for our contingency planning, consequence management, and continuity of operations services. We have effectively collaborated with federal and corporate organizations to define and understand their core functions and processes and to identify critical business infrastructures. These include essential personnel, operations, facilities, and information systems, as well as life safety systems, safe haven areas, and security technology.

One of our core competencies is a well-honed ability to research, interpret, and assist in the execution of – and compliance with – the emerging thicket of federal rules, regulations, policies, and guidelines issued by several governments in the area of Homeland Security. All our recommendations comply with current policy, doctrine, and operational guidelines.

The firm has developed depth and expertise in the most critical element of security; the trade-off. We know perfect security is impossible; consequently, we assist institutions in balancing the expense, convenience, efficiency, and restrictions that inevitably attach themselves to any security system. By objectively assessing the threat environment and developing a profound appreciation for the client's institutional mission, our recommended trade-offs and related procedures provide a tangible benefit to the client organization. To ensure an executable security strategy, McManis & Monsalve security experts work with executives, scientists, managers, and technical personnel to establish operations and procedures that are aligned with – and enhance – the institution's goals and mission.

Given the uncertainty of emerging terrorist and criminal threats, many of our clients require a quick qualitative assessment of the vulnerability to existing operations, personnel, facilities, and assets. Because of the transitory and evolutionary nature of these threats and their uncertain duration, we have developed highly effective approaches to risk reduction by emphasizing reorganization of operational functions and procedures. Our Threat, Risk and Vulnerability Assessment Teams scrutinize business and operational practices to identify opportunities to reduce exposure to internal or external attacks, whatever their motivation and scope. Our experience and research proves that the application of physical security measures and technology without an organizational realignment results in significant expenses without a tangible improvement in real asset protection.

Other clients require in-depth Threat, Risk, and Vulnerability Assessments that can meet the rigorous standards imposed by law and regulation, as has been the case with government funded and supervised biomedical research facilities. Our record in the area speaks for itself and our partnerships with internationally recognized firms such Oudens + Knoop Architects (Washington, D.C.), Weidlinger Associates (New York City) and the Mercyhurst Center for Intelligence Studies adds unparalleled depth to our services.

Research conducted by our senior consultants – whose expertise in the field is widely acknowledged in academic, corporate, and governmental sectors – created the knowledge

and processes needed to evaluate security, tools, systems, technologies, and practices. Without the application of this process and experience, organizations are likely to apply significant financial and human resources and not achieve the desired level of protection.

In the end, we internalize our client's priorities and collaborate with key personnel to execute the best strategy to protect the enterprise and ensure its continuity.

To ensure the efficiency of an organization's security strategy, we work with the executives, managers, and technical personnel to establish a continuous review and improvement process that is aligned to the organization's specific business practices. Our security professionals provide technical assistance in conducting security surveys and assessments, training, development of design and policy solutions, and ongoing monitoring programs.

Our goal is to help our clients develop and implement programs that work; that are cost-effective and sensitive to their needs; and that can be sustained.

Our clients' return on their security investment improves because we help them:

- **Standardize security assessment methodologies**
- **Prioritize security needs and identify appropriate mitigation strategies**
- **Institutionalize security strategies into the organization's administrative and operational infrastructure**
- **Optimize security performance**

We work hand-in-hand with our clients to plan, develop, and deploy an end-to-end solution for protecting their organization's assets. This methodology ensures effective collaboration with our clients to proactively evaluate which assets they need to protect, identify and assess likely threats, evaluate security policies and controls, and test and improve security processes to ensure the best value.

EXPERTISE

Our security professionals bring extensive governmental and corporate executive experience, as well as internationally recognized expertise in the field. They excel in applying the state of the art knowledge and technology to problems in diverse fields. Our staff includes persons with graduate degrees in fields as diverse as industrial psychology, risk management, physical security, and public policy analysis. The innovative vision and breadth of experience this multi-disciplinary group brings to the table ensures that our services are effectively tailored to the client's own dynamic environment.

SERVICES

Our mission and objective is to help governmental and corporate clients secure their enterprise and ensure the continuity of their operations, whatever threat they might face and whatever rubric is used to identify the challenge. The professional experience of our senior consultants includes executive, governmental, and corporate assignments with specialties in:

- Consequence Management
- Contingency Planning
- Continuity of Operations Planning
- Counterintelligence
- Crisis Management
- Counterterrorism and Force Protection
- Critical Infrastructure Protection Planning
- Information Security (INFOSEC) and Intellectual Property Protection
- Intelligence Research and Analysis Support
- Insider Threat Evaluation
- Operations Security (OPSEC)
- Physical Security and Security Technology Plans, Programs and Evaluation
- Scenario Development & Table Top Exercises
- Social Network Analysis
- Security Program Development & Reengineering
- Threat Assessment, Evaluation, and Mitigation
- Threat Modeling
- Vulnerability & Risk Assessment
- Wargaming and Table Top Exercises and Evaluation
- Complex Investigations and Corporate Compliance Programs (Sarbanes-Oxley Act)
- Security Training & Awareness Programs

Our approach and execution is consistent with the latest governmental regulations, policy, and guidance.

THREAT, RISK AND VULNERABILITY ASSESSMENTS

The Threat, Risk, and Vulnerability Assessments (TRVAs) provided by McManis & Monsalve are based on the latest governmental guidance and accepted standards of corporate risk management practice. This experience is predicated on the fact that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it.

Our firm's approach and its methodology are based on a systematic and analytical process that evaluates the probability that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack. Our Risk Management strategy includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment.

One of the most significant challenges our firm faces in this area is the absence of a common government-wide risk assessment methodology, particularly against terrorist threats (which – given their asymmetrical nature – are generally not amenable to current risk management practices) that are based on known trends and deterministic analysis. This problem is compounded by the absence of common framework of terminology and the transfer of best practices within the U.S. government. While TRVAs are routinely conducted by the Department of Defense, Department of Energy, Department of State, Department of Justice, Department of Health and Human Services and others, the method reflects departmental priorities, culture, and common practices.

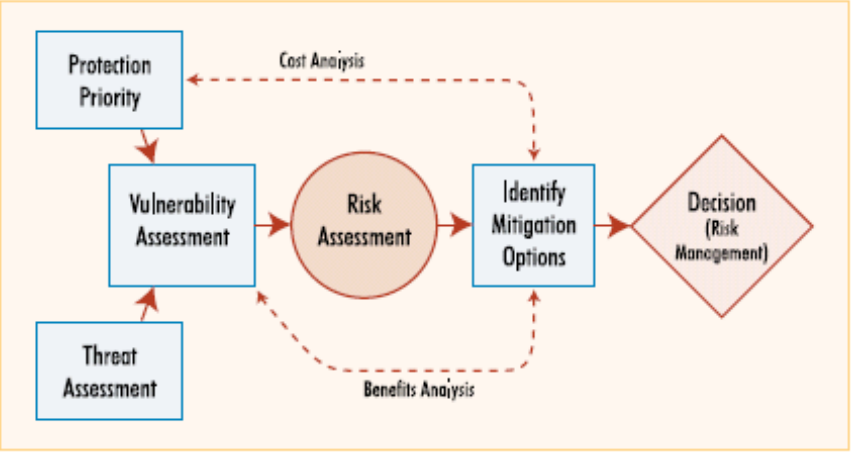
Our research has fused these disparate procedures into one that reflects the best practices across the government. Our efforts are also informed by emerging regulatory guidance that includes:

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001;
- Homeland Security Act of 2002;
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002;
- Agricultural Bioterrorism Protection Act of 2002;
- Terrorism Risk Insurance Act of 2002; and
- Department of Homeland Security, including the Federal Emergency Management Agency Multi-hazard Risk Management Series.

Following the attack of September 11, 2001 the urgency to conduct vulnerability assessments involving terrorist concerns has increased significantly. The protection of civilian population from acts of terrorism has become a major national priority. Our firm's research indicates that regulatory mandates in this area are likely to expand and harden, especially if we have another major terrorist event.

The insurance, finance, and regulatory communities are also likely to modify theirs to the issue of terrorism risk management in evaluating and managing of risk exposure for enterprises. Lenders are likely to require TRVAs as a pre-condition for purchase and construction loans. Insurers will change their premiums to risk and rewarding effective mitigation.

In general, McManis & Monsalve's methodology follows the FEMA Risk Reduction Process noted in the following graphic:



The first step of the process to assess risk to terrorist attack is to identify the relative importance of the people, business activities, goods, and facilities involved in order to prioritize security actions. The second step is to define and understand the core functions and processes of the business or institutional entity. The third is to identify critical business infrastructure, which includes essential components such as key people, functions, facilities, information systems and data processing equipment and nodes, as well as life safety systems, safe haven areas, and the safety & security systems that integrate and monitor this areas.

Our firm's TRVAs have proven their value as decision support tools that can assist organizations in security-program planning. Our approach allows organizations to identify and evaluate threats based on various factors, including capability and intentions, as well as the potential lethality of an attack. By identifying and assessing threats, organizations do not have to rely on worst-case scenarios to guide planning and resource allocations. Worst-case scenarios tend to focus on vulnerabilities, which are virtually unlimited, and would require extraordinary resources to address. Therefore, in the absence of detailed threat data, it is essential that a careful balance exists using all three elements in preparing and protecting against threats.

While some of our engagements have been limited to Threat Assessments only, the fact remains that it is not possible to identify every threat, nor is it possible to have complete information about the identified threats. As a consequence, we generally recommend completion of the Risk Management Cycle, which also includes vulnerability assessments and criticality assessments.

The vulnerability assessment identifies weaknesses that may be exploited by criminals and terrorists and recommends options/strategies to eliminate or mitigate those weaknesses. A criticality assessment is designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a facility. Criticality assessments are important because they provide a basis for prioritizing which assets and structures require higher or special protection from an attack.

EXAMPLES OF OUR WORK

Walter Reed Army Medical Center

Installation Force Protection/Anti-terrorism (AT/FP Plan)

Walter Reed Army Medical Center is a medical care and research facility for the U.S. Army located on a 112 acre campus in the Northwest area of Washington, DC. Many of the neo-Georgian Buildings are eligible for listing on the National Historic Register, and much of the site is a Historic District.

The AT/FP Plan consisted of a Threat, Risk and Vulnerability study of the overall site and 21 mission-essential buildings using the Unified Facilities Criteria (UFC) of the Department of Defense as the metric for vulnerability.

As an urban, densely-developed complex, the installation cannot meet many of the desired standoff distances of the UFC. Alternative mitigation measures were therefore recommended.

The AT/FP Plan also includes an operations Antiterrorism Plan and an Emergency Management Plan.

The National Institutes of Health (NIH)

Main Campus, Bethesda, Maryland

The Main Campus of the NIH is a 310 acre property north of the Bethesda, MD Central Business District in the suburban Washington, DC area. The campus now employs over 18,000 persons, has over 70 buildings and over 7.3 million gross square feet of Occupiable buildings including a hospital, biomedical research laboratories, offices, animal holding and many other support facilities.

McManis & Monsalve Associates assisted the NIH in responding to the increased security required for the campus by the Office of the Inspector General of the Department of Health and Human Services (DHHS). This included developing perimeter security with personnel and vehicle barriers, screening for vehicles and visitors and other physical and operational security measures.

McManis & Monsalve prepared the Threat and Risk Assessment for the campus and for the leased properties in the Montgomery County area, including the development of comprehensive policies for providing physical security.

Rocky Mountain Laboratories, Hamilton, MT

A 33 acre campus of the National Institute of Allergy and Infectious Diseases (NIAID), and the site of a new research building containing Bio Safety Level (BSL)-3 and 4 containment facilities.

McManis & Monsalve Associates performed a Threat and Risk Assessment and assisted the NIH management in developing security operations onsite and assisted the NIH in developing the physical security policies, guidelines and criteria for the site, including perimeter and access control.

Research Triangle Park, North Carolina

A 509 acre campus for the National Institute of Environmental Health Sciences (MIEHS) shared with the headquarters of the Environmental Protection Agency (EPA).

McManis & Monsalve Associates performed a Threat and Risk Assessment and assisted the NIH management in developing security operations onsite and assisted the NIH in developing the physical security policies, guidelines and criteria for the site, including perimeter and access control.

NAID Bioterrorism Research RBL and NBL Grantees

University of Pittsburgh: Regional Biocontainment Laboratory University of Pittsburgh; Threat, Risk and Vulnerability Assessments by McManis & Monsalve Associates

University of Texas Medical Branch - Galveston: Threat and Risk Assessment for the Galveston National Laboratory; Threat, Risk and Vulnerability Assessments

University of Alabama at Birmingham: Threat and Risk Assessment for the Southeast Biosafety Laboratory Alabama Birmingham; Threat, Risk and Vulnerability Assessments

Perimeter Security for the Nuclear Regulatory Commission's Headquarters Facility

Following the events of September 11, the Nuclear Regulatory Commission ordered a study to determine the optimal physical security solution for the facility's perimeter. McManis & Monsalve Associates conducted a Threat, Risk and Vulnerability Assessment and delivered a report outlining physical security recommendations for the Headquarters Facility. These included a design for a perimeter security system compatible with the existing topography and the criteria established by the using Agency and GSA. These recommendations were then turned over to an architectural firm for implementation.

City of Hamilton, Montana, Vulnerability & Risk Assessment of Water and Wastewater Facilities

McManis & Monsalve Associates assisted the City in conducting an evaluation of the reliability and integrity of the potable and waste water system provided by the City of Hamilton. The Public Health, Security and Bioterrorism Preparedness and Response Act of 2002 required the City of Hamilton to certify the completion of a vulnerability assessment and emergency response plan, and the submit copies of the assessments to the Environmental Protection Agency [EPA]. McManis & Monsalve conducted this assessment and evaluated the Hamilton Water Works susceptibility to potential threats and identified corrective actions that could reduce or mitigate the risks from adversarial actions (e.g., vandalism, insider sabotage, terrorist attack, etc.) The Assessment was successfully completed and submitted to the EPA.

Department of Homeland Security, Office of Infrastructure Protection, and Office of Cybersecurity and Communications, Critical Infrastructure Warning Information Network Need and Mission Risk & Threat Assessment Study

The DHS Office of Infrastructure Protection (IP) is responsible for protecting the nation's Critical Infrastructure and Key Resources (CIKR). DHS IP provides coordination for rapid recovery of the CIKR during events of national significance. The Office of Cyber Security & Communications (CS&C), also within DHS, is responsible for securing and ensuring the availability of our nation's cyber and telecommunications infrastructure. Both IP and CS&C are responsible for preventing and minimizing disruptions to our critical information infrastructure in order to protect the public, economy, government services, and the overall security of the United States. McManis &

Monsalve Associates was tasked with conducting a comprehensive Risk and Threat Assessment of the U.S. Critical Infrastructure Warning Information Network. The assessment looked at the probability and risk of the Public Switched Network (PSN) going down totally from a cyber-attack, and the probability and risk of the Internet going down from a cyber-attack. In order to conduct the study the consulting team had to develop a complex PSN/Internet cyber threat model that could determine the probability that an attack would knock out the PSN or Internet in the United States. With the model test data in hand; the team then developed profiles of threat groups (nation states, organized groups, individual actors, etc.) that have the motive and capability to perpetrate cyber-attacks. These threat group profiles were used to drive test scenarios in our cyber threat model and provide an overall picture of the probability of our PSN and Internet completing failing due to cyber-attacks. The Assessment was used to help inform policy and infrastructure decisions including the development of high level requirements used to identify and evaluate alternative approaches to contingent connectivity, the Identification of other technologies, market and government capabilities that could fulfill the need for a network independent of the PSN and Internet, and identification of who in DHS should have organizational responsibility for the requirement.

Capitol Trailways Antiterrorism Security Assessment

McManis & Monsalve Associates conducted a comprehensive threat assessment that evaluated criticality, vulnerability, and risks to employees, customers, operations and assets of this national corporation. Specifically, the assessment addressed threats, risks and vulnerabilities involving passengers; the general public; bus terminals or depots; employees (to include drivers); buses (both operational and stationary); and luggage and packages. The assessment addressed possible direct attacks against Capitol and attacks in which terrorists would utilize Capitol's assets to achieve a violent end. For example, the possibility that a terrorist could place a bomb on a bus designed to blow up once it was parked next to a building in New York City or a casino in Atlantic City. Based on the threat assessment, legal liability, and operational efficiency of Capitol Trailways, McManis & Monsalve developed internal procedures/protocols. The protocols addressed incident response to various threat and/or terrorist situations, communications, and security procedures and were specifically tailored for the functional areas of: bus drivers, management, and the Capitol office staff.