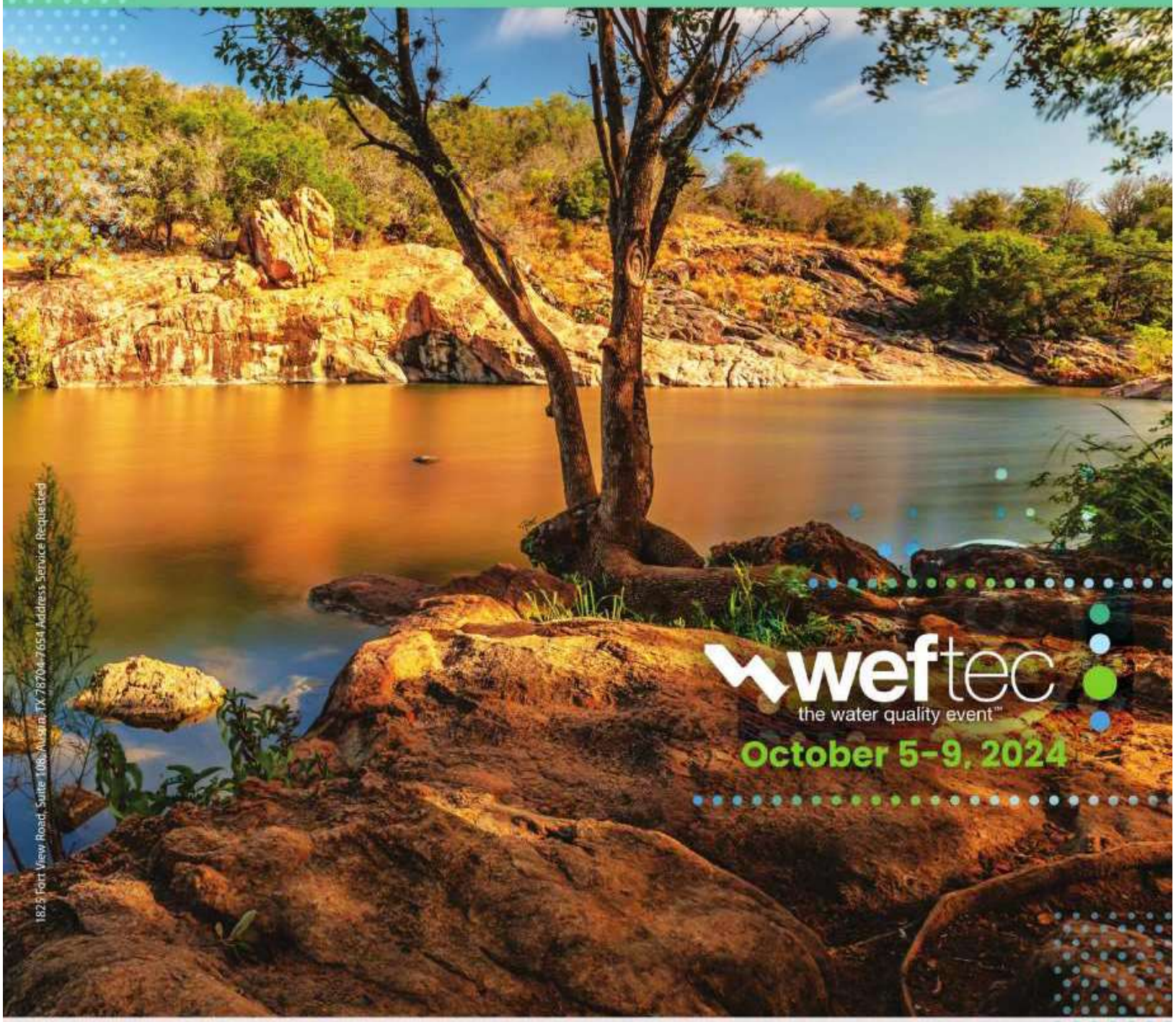
TexasWET

LEADERSHIP FOR THE WATER ENVIRONMENT IN TEXAS

Official Publication of the Water Environment Association of Texas

Issue 4 • 2024



1825 Fort View Road, Suite 108, Austin, TX 78704-7654 Address Service Requested

Water Environment Association of Texas

INSIDE PLANT SPOTLIGHT: THE PENINSULA WRP | SECTION REPORTS

UNDER ATTACK: BUILDING A SECURITY PROGRAM TO PROTECT CRITICAL INFRASTRUCTURE

By Robert W. Starnes

Cyber penetrations against water treatment facilities, increased physical security attacks against the electric grid, and catastrophic attacks against houses of worship, critical infrastructure sectors within the United States remain targets of attacks.

Reviewing organizational security postures to mitigate vulnerabilities is paramount. Literature about varying aspects of how to build security programs could fill many libraries. This article is not meant to serve as a comprehensive guide addressing all security disciplines aimed primarily at prevention and protection against malicious acts. Instead, it provides a high-level view of the major components for developing a reliable security program.

Preventing and defending against malicious actors within various critical infrastructure sectors generally requires significant risk management strategies, assessing/mitigating vulnerabilities, planning, security education/awareness, and budgetary considerations. Of course, an organization's top priority must be protecting its most valuable assets – human lives.

CRITICAL INFRASTRUCTURE SECTORS

Critical infrastructures include assets, network systems, facilities, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. There are four designated lifeline functions – transportation, water, energy, and communications, meaning that their reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors.[i]

The U.S. National Infrastructure Protection Plan[ii] (NIPP) addresses resiliency for sixteen (16) critical infrastructure sectors, including the water (and wastewater sectors). The NIPP encourages stakeholders to manage risks from significant threats and hazards to physical and cyber critical infrastructure by:

- Identifying, deterring, detecting, disrupting, and preparing for threats and hazards to the Nation's critical infrastructure.
- Reducing vulnerabilities of critical assets, systems, and networks; and
- Mitigating the potential consequences to critical infrastructure of incidents or adverse events that do occur.

The success of this integrated security approach depends on leveraging the full spectrum of capabilities, expertise, and experience across the critical infrastructure community and associated stakeholders.

Presidential Policy Directive 21[iii] (PPD-21) notes: *The NIPP is aligned with the goal of PPD-8, National Preparedness, of "a secure and resilient Nation with the capabilities required across the whole community to* ***prevent, protect against, mitigate, respond to****, and* ***recover*** *from the threats and hazards that pose the greatest risk."*

TEXAS SECURITY ROADMAP

Just as roadmaps are essential to travelers undertaking lengthy journeys, security professionals protecting our nation's critical infrastructures are aided by proven processes to achieve the prevention and protection goals. Except for limited regulatory requirements, such as Federal Energy Regulatory Commission (FERC), Nuclear Regulatory Commission (NRC), and others Federal, State, and local regulatory bodies, security professionals operating within government, and private entities generally follow security advice contained within industry standards and historical best practices.

I was recently asked what guidelines I use when developing a security program within the water sector. My response was simple, foundationally, I follow framework contained within the Texas Governor's Office of Homeland Security's Strategic Plan of 2021-2025[iv].

SECURITY PROGRAM COMPONENTS

Basic hierarchal security components to consider when reviewing, developing, and implementing a sustainable security program include:

1. Threat Assessment
2. Risk Management
3. Facility Protection
4. Drone Program
5. Procedural Security
6. Construction Security
7. Surveillance Detection
8. Executive Protection
9. Investigations
10. Protective Intelligence
11. Protective Liaison
12. Cybersecurity
13. Security Awareness Training
14. Crisis Management Planning

1. ASSESSING THREATS

Identifying threat and hazards and assessing risks helps organizations answer the following questions:

- What threats and hazards can affect an organization?
- If they occurred, what impacts would those threats and hazards have on the organization?
- Based on those impacts, what capabilities should an organization have?

The Threat & Hazard Assessment process includes:

- Identifying threat/hazard categories and adversaries.
- Assessing intent and motivation of each adversary.
- Assessing capabilities of each adversary.
- Determining frequencies of past events.
- Estimating threat relative to each critical asset.

Adversarial/Human Caused Categories include:

- Terrorism
- Kidnapping

- Theft
- Burglary
- Robbery
- Explosives attack
- Vandalism
- Fraud
- Sabotage
- Cyber incident
- School and workplace violence
- CBRN attack

2. MANAGING SECURITY RISKS

Security Risk Management (SRM) is the process of assessing, and analyzing relationships between security risks and impacts to an organization. SRM integrates assessing threats, vulnerabilities, and the value of the asset to the risk of compromise/loss, against the cost of implementing security countermeasures to maintain organizational strategic goals.

Risk = Asset (Impact) x (Threat x Vulnerability)

Implementation of security countermeasures to achieve an acceptable level of risk at an acceptable cost can be achieved by a systematic and proactive approach to support toward organizational strategic goals and minimize negative impact to the entity and public assets via:

- Risk Avoidance;
- Risk Transfer; or
- Risk Mitigation.

3. FACILITY PROTECTION

Physical security is a mainstay for protecting personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution. Physical security capabilities are supported and achieved by "identifying, assessing, and mitigating vulnerabilities through the deployment of physical protective measures," and "deploying protective measures commensurate with the risk from an incident and balanced with the complementary aims of enabling commerce and maintaining the civil rights of citizens."

The physical security concept is to create a layered or "tiered" defensive system to delay intruders. The tiered defensive system consists of layers or zones of increasing defense starting at the outer perimeter and ending with the safe haven area. It provides both a deterrent to hostile acts and a response time for local security forces using physical security barriers and access denial systems, while incorporating design elements to achieve the following four capabilities:[1]

DETER

Deterrents can include signage, physical barriers (e.g., hardlines, gates, etc.), or more psychological deterrence (ex. video surveillance), but all serve a similar purpose in signifying that a site is protected.

DELAY

Delay is accomplished using barriers and set back. Perimeter fences, hardlines, walls, forced entry (FE) doors and windows, and safe havens/areas are examples of barriers. Since any barrier can eventually be defeated, the goal is to provide adequate time for personnel to retreat to the safe haven/area, and for local first responders to intervene.

DETECT

Detection alerts the selected personnel and/or local authorities to unauthorized access or actual intrusion. Without detection, the element of response is removed, and delay is no longer a significant concern to the attacker. Detection encompasses entry control and surveillance systems as well as intrusion alarms with monitoring and/or notifications.

RESPONSE

Response elements or units attempt to interrupt or neutralize the intrusions or attacks. The response element is enhanced by communications and assessment equipment, such as access control and intrusion detection systems, surveillance video cameras, radios, intercoms, and emergency annunciating systems.

4. DRONE PROGRAM

An aerial drone program can offer critical infrastructure stakeholders multiple protective uses, including property mapping, facility modeling, using drones as a first responder tool, project management, engineering structure inspections, vulnerability assessment, lighting surveys, surveillance choke-point identification, emergency management, health & safety, environmental protection, and many other uses.

Mapping – Stakeholders can use in-house or contracted pilots to fly sorties for capturing high-resolution GIS tagged images.

Modeling – Internal facility 3D modeling can be quickly shared with first responders including law enforcement, security, and emergency management professionals dispatched to facilities to learn building layouts more quickly (i.e., barricade situations, fire and hazmat response, etc.).

Digital Dashboards – A security digital dashboard can be a helpful one-stop platform, linking security cameras via IP addresses, visually identifying security equipment locations, and other important documents for quick access by security forces and management team members (i.e., incident reports, contracts, emergency action plans, building/utility schematics, maintenance schedules, etc.).

5. PROCEDURAL SECURITY

Procedural Security is the identification, modeling, establishment, and enforcement of security policies and/or procedures that regulate the usage of system processes including:

1. Insider Threat
2. Travel Security
3. Access Control Management
4. Mail/Parcel Deliveries
5. Incident Reporting and Analysis
6. Operational Security (OPSEC) is a security and risk management process with the goal of protecting sensitive information (written or verbal) by unintentional or unauthorized disclosure or by illegal means for criminal intent (i.e., espionage, terrorist planning, illicit financial gain, etc.), including sensitive document processing, storage and/or destruction.

7. CONSTRUCTION SECURITY

Granting access for contractors to critical infrastructure sites is a serious matter. A security program should ensure contractor vetting as a condition to authorizing access. Record checks help to evaluate if contract employees are suitable for employment, (i.e., reliable, trustworthy, of good conduct and character), thus reducing the likelihood of

CLICK HERE TO RETURN TO TABLE OF CONTENTS

hiring someone with a history of behaving in a threatening, violent, or untrustworthy manner. Given the importance of protecting staff and critical infrastructure facilities, consideration should be given to establishing a reasonable baseline for reaching an adjudication determination for allowing contractor authorized access based on criminal history.

Record Check Options:

a) *DPS Secure Website*
The Texas Department of Public Safety (DPS) Secure Website consists of the state's Computerized Criminal History System (CCH). The CCH System is the statewide repository of criminal history record information reported by all arresting agencies in the state. The data in the CCH consists of arrest, prosecution, and disposition of the case for persons arrested for Class B Misdemeanor or greater violations of Texas statutes. This database can be accessed by non-commissioned peace officers.

b) *National Crime Information Center (NCIC)*
The NCIC is a computerized index of missing persons and criminal information and is designed for the rapid exchange of information between criminal justice agencies. Approved users access the NCIC computer located at FBI headquarters through regional or State computer systems or with direct tie-ins to the NCIC computer.

In 2016, the FBI authorized the use of NCIC for vetting contractors seeking access to critical infrastructure facilities (CIF) (see attached NCIC MOU draft). Under this FBI memorandum, CIF owners seeking access to NCIC for vetting contractors must be approved for the following actions:

1) Request authorization to become a "terminal agency" to house an NCIC computer terminal; or,
2) Enter a Memorandum of Understanding (MOU) with a law enforcement agency authorized access to the NCIC database. Given the NCIC's restriction of sharing criminal histories with non-law enforcement personnel, a "green light" "red light" verification system must be developed allowing the law enforcement agency to notify the CIF owner of contractor access eligibility/denial based on the CIF's pre-established access adjudication standards.
3) The responsible law enforcement agency must request a specific originating number (ORI) to be used specifically for NCIC checks conducted for CIFs. The ORI/CIF is to be used for all contractor vetting record checks.
4) The CIF must develop a redress procedure. The redress procedure allows contractors who have been denied access based on the CIF's adjudication standards an ability to seek redress through the originating agencies who have entered arrests and/or judicial actions for the contractor personnel into the NCIC database.

8. SURVEILLANCE DETECTION

Terrorists are generally most vulnerable to discovery during their pre-attack surveillance phase. The investigation for the 1998 bombings of the two U.S. embassies in East Africa revealed Al-Qaeda operatives surveilled their targets nine-months prior to their attacks. Thus, detection of "pre-operational" surveillance is highly effective in disrupting or mitigating a terrorist attack.

9. EXECUTIVE PROTECTION

Also referred to as close protection, Executive protection (EP) relates to security and risk mitigation measures taken to ensure the safety of executives and other individuals who may be exposed to elevated personal risk because of their employment, high-profile status, net worth, affiliations or geographical location.

Executive Protection may include:

1. Site Advances
2. Detail Agents
3. Shift Leader
4. Agent-in-Charge
5. Motorcade operations

10. INVESTIGATIONS

Establishing an investigations program is an important security element. Generally, investigative programs fall into two main categories.

1. Criminal Investigations
2. Personnel Investigations
   a. Pre-employment suitability
   b. Employee misconduct or malfeasance

11. PROTECTIVE INTELLIGENCE

The goal of Protective intelligence is to analyze and synthesize information that is of tactical, operational, or strategic value to protect assets. Protective Intelligence is a vital component incorporated into the multi layers of facility protection and classified as a core capability for facility protection and crisis management contained within the National Planning Framework. It is vital that a security program includes establishing close relationships with government agencies tasked with collecting and disseminating threat intelligence.

Sources of threat intelligence for critical infrastructure in the State of Texas include:

a) Joint Terrorism Task Force (JTTF)
According to the Federal Bureau of Investigations (FBI), in the United States, the Joint Terrorism Task Forces are locally based multi-agency partnerships between various federal, state, and local law enforcement agencies tasked with investigating terrorism and terrorism-related crimes, led by the FBI and U.S. Department of Justice.

b) Fusion Centers
According to DHS, Fusion Centers are state-owned and operated centers that bring two-way intelligence and information flow between the federal government and our State, Local, Tribal and Territorial (SLTT), federal and private sectors in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information.

c) InfraGard
InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for protection of U.S. Critical Infrastructure.

d) Department of Homeland Security/ Cybersecurity and Infrastructure Security Agency (CISA)
CISA is the operational lead for federal cybersecurity and the

national coordinator for critical infrastructure security and resilience. CISA is designed for collaboration and partnership to reduce risk to the nation's cyber and physical infrastructure.

e) United States Secret Service (USSS)
The U.S. Secret Service' National Threat Assessment Center (NTAC) was established as a component of the Secret Service in 1998 to provide research and guidance in direct support of the Secret Service protective mission, and to others with public safety responsibilities.

f) Overseas Security Advisory Council
The Overseas Security Advisory Council (OSAC) is a public-private partnership between the U.S. Department of State's Diplomatic Security Service (DSS) and security professionals from U.S. organizations operating abroad. Together, OSAC members share timely security information and maintain strong bonds for the protection of U.S. interests overseas.

12. PROTECTIVE LIAISON

Building and maintaining mutually beneficial relationships, facilitating information sharing, communications and coordinating activities among people, agencies and organizations categorized as a core capability for facility protection and crisis management contained within the National Planning Framework.

13. CYBERSECURITY

Establishing and maintaining a robust cybersecurity program is critical for protecting all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

14. SECURITY AWARENESS TRAINING

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of human and physical assets of that organization. Employees and contractors can serve as the eyes and ears of a BRA-wide security effort.

Security Awareness Guidance Topics

- Personal Security
- Sexual Assault Prevention
- Detecting Sexual Abuse
- Countering Terrorism
- Surveillance detection
- Reporting suspicious activities
- Reporting suspicious packages
- Workplace violence (Active Attacker)
- Gun Violence Prevention
- Street Security Tips
- Travel Security
- Pet Safety
- Operational Security
- Residential Security
- Automobile Security
- Mail Protection
- Child Abuse Prevention
- Children Safety Tips
- Children Safety Tips
- Domestic Staff Security
- Residential Phone Security
- Emergency Preparation Planning
- Cybersecurity

Available Security Related Training Resources for Critical Infrastructure

1) **Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (DHS/CISA)**
Protective Security Advisors (PSAs) are trained subject matter experts in critical infrastructure protection and vulnerability mitigation. PSA's facilitate local field activities in coordination with other DHS offices and federal agencies. They also advise and assist state, local, tribal, and territorial (SLTT) officials and critical infrastructure owners and operators, and provide coordination and support in times of threat, disruption, or attack.
2) U.S. Secret Service (USSS)
3) Federal Bureau of Investigations (FBI)
4) Federal Emergency Management Agency (FEMA)
5) Environmental Protection Agency (EPA)
6) Texas Engineering Extension Service (TEEX)
7) Texas Department of Public Safety (DPS)
8) Texas Homeland Security
9) Texas Commission on Environmental Quality (TCEQ)
10) Texas School Safety Center (Texas State University)
11) American Society of Industrial Security (ASIS)

15. CRISIS MANGEMENT PLANNING

Crisis management is a dynamic process beginning well before the critical event and extends beyond its conclusion. Crisis management is the process of preparing for, mitigating, responding to and recovering from a crisis event. Effective crisis management requires a method to account for employees and visitors, a method for incident command, and a specified communication system. It is critical for an organization to develop crisis

Preventing and defending against malicious actors within various critical infrastructure sectors generally requires significant risk management strategies, assessing/mitigating vulnerabilities, planning, security education/awareness, and budgetary considerations

CLICK HERE TO RETURN TO TABLE OF CONTENTS

management plans and practice the plans via drills and tabletop exercises.

Crisis management planning for malicious attacks may include responses for:

- Emergency Evacuation Plan
- Terrorist Threat Plan (ThreatCon)
- CBRN Plan
- Bomb Threat Plan
- Suspicious Package Response Plan
- Active Attacker Plan
- Civil Disturbance Plan

CONCLUSION

Given seemingly deteriorating worldwide security posture, now is the time to review, and establish robust organizational security programs. Staff and the public are relying on critical infrastructure owners and operators to protect and maintain operations from malicious attacks.

REFERENCES

[1] U.S. Dept. of State, Office of Foreign Building Operations, (2000). Compendium of Physical Security Design Standards v2. Other public domain resource information provided by the U.S. Homeland Security/CISA, U.S. Justice Dept., FBI, U.S. Secret Service, U.S. Dept. of State, InfraGard, and Texas Dept. of Public Safety,

[i] DHS/CISA, (2019), A Guide to Critical Infrastructure Security and Resilience.

[ii] Presidential Policy Directive 21. (2013) Infrastructure Security and Resilience.

[iii] Presidential Policy Directive 8. (2011). National Preparedness.

[iv] Texas Governor's, Texas Homeland Security Strategic Plan 2021-2025.

ABOUT THE AUTHOR:

Robert W. Starnes is currently the executive security manager for the Brazos River Authority. After twenty-five years career, Robert retired from the U.S. Department of State, Diplomatic Security Service with expertise in international counterterrorism, counterintelligence, investigations, executive protection and protective security for multiple U.S. diplomatic missions throughout the world. He also served as a state trooper with the Texas Department of Public Safety. Robert is an author and public speaker. His writings include *Dictators and Diplomats – A Special Agent's Memoir and Musings* and *On the Shoulders of Giants – Inspiration by Virtues*. He and his spouse of 40 years reside in San Marcos, Texas. ●

Reviewing organizational security postures to mitigate vulnerabilities is paramount. Literature about varying aspects of how to build security programs could fill many libraries.