A Strategic Blueprint

for

World Class Seaport Security

Prepared by: Michael Mc Nicholas

Phoenix Group®

With few exceptions, the ports of the world are increasingly under threat of penetration, manipulation, and usage by drug smugglers, stowaways, cargo thieves, pirates, and terrorists. Targets of these criminal elements include the terminals, vessels, cargo, containers, equipment, and personnel. In addition to concerns regarding the rising number of incidents of violent piracy and waves of stowaways/refugees in the past couple years, ports in these post-11 September 01 times must also face the looming specter of terrorist attacks involving weapons of mass destruction or of a vessel being used by terrorists as a conveyance or an instrument of destruction. To effectively deter or deny these threats, ports must develop a security strategy that identifies the potential threats, defines critical assets and information, integrates security resources and capabilities, and ensures the successful design, implementation and management of a world class seaport security program.

The most comprehensive and effective seaport security program is one based on the military concept called "Defense-In-Depth." Applied to a seaport, this concept involves the design and establishment of a series of security "rings" around and in the port, as well as encircling critical assets within the port (such as cranes, vessels, etc.). The number of security rings established and the specific components (security systems and measures) of each ring will vary and depend upon the port's layout and operations, its assets, and the level, type, and duration of the threats. While the rings themselves are permanent or long-standing, the individual components within the rings may be long term or temporary; as in the case of measures implemented to address a crisis situation or a short term threat. These security rings should be layered and integrated, but capable of functioning independently. Security ring components include physical security measures, procedural security standards, specialized assets, and personnel resources. It is important to appreciate that no one component can efficiently or effectively accomplish the overall task without the support of the others. As an example, while a security officer may be deployed at an entrance gate to control access, if there is no written or defined access control procedure or an identification badge system in-place he can not effectively perform this function. While many of the component systems and measures deployed in a security ring configuration may be permanent, others may be temporary, such as those enacted during a labor strike or terrorist alert. The temporary implementation or activation of special security components or procedures due to heightened threats should be preplanned and part of an overall Threat Condition Status system and detailed in the Security Standard Operating Procedures Manual and Emergency Action Plan. A brief outline of a world class seaport security program -- one which is designed for a multi-threat environment and utilizes layered security rings -- includes the following concepts:

1. EXTERNAL SECURITY RING

1.1. ***Intelligence Operations*** -- The continual tasking, collection, analysis, dissemination, and evaluation of strategic and tactical intelligence & information from confidential informants (persons associated with or inside criminal and terrorist organizations) and sources of information in the communities and regions surrounding and inside the port (such as truck drivers, warehouse laborers, documentation clerks, cargo surveyors, open press, news reporters, etc.) to provide advance indications and warnings of evolving and future criminal activities or threats targeting the port are key tenets of the port security strategy. In many cases, the success of the port security program depends upon the ability to receive advance knowledge of planned criminal/terrorist activities and direct or manipulate events so that these situations are neutralized or contained outside the port or within one of the security rings.

1.2. ***Government and Law Enforcement Liaison*** -- The establishment of active and ongoing relations with and support from national government agencies, such as the Police, Customs, Military, and Intelligence services is a fundamental necessity. Also desirable are working-level contacts with international and non-host country law enforcement and intelligence agencies, such as INTERPOL and foreign Customs services. These entities can provide vital information concerning activities by transnational criminal and terrorist organizations that may target the seaport or a vessel or its cargo.

2. PERIMETER SECURITY RING

2.1. ***Physical Security Barrier & Illumination*** -- The entire land boundary of the port is identified and protected by a wall or fence no less than eight feet in height and topped with three strands of barbed wire or baled concertina wire. The wire topping should be secured to arms that are angled outward at 45 degrees. If the perimeter barrier is fencing, then it should be constructed of either of "climb-resistant" stretched steel or 9-gauge chainlink wire mesh, with two-inch openings, and secured at the bottom with metal tubing or a concrete footing, to deter under the fence ingress.

Photo 15.1. – Sample perimeter barrier

The level of illumination along the perimeter barrier should be no less than 2-foot candles at ground level (similar to the level of lighting in a stadium), projecting 10 feet inside the barrier and 20 feet outside the barrier. This same lighting standard should be met in cargo and container staging areas, along the berths, and on the exterior of buildings and warehouses. Good lighting is arguably the most effective and least expensive measure of deterrence against cargo pilferage, container theft, and other similar violations.

2.2. ***Waterside Security Measures*** -- A security launch with armed security officer (s) should patrol along the berth and in nearby waters to deter or prevent unauthorized approach and access on the waterside of the port by stowaways, smugglers, pirates, terrorists, etc. Increasingly narcotics trafficking organizations are using SCUBA divers to attach drug-laden torpedoes/boxes to the hulls and undersides of vessels. If this threat is suspected, the port security program should include the use of underwater security patrols (SCUBA), an anti-diver system, or the installation of underwater CCTV cameras. Likewise, drug smuggling and professional stowaway organizations utilize small boats or launches to transport their stowaways, drug couriers, and contraband to the waterside of the vessels for lading. Moreover, as demonstrated by the attack on the USS COLE in Yemen, terrorists utilize small launches and port services vessels to attack large vessels while in port. The 24-hour security patrol ensures that threats from the waterside are deterred or prevented.

Photo 15.2. – Security Launch patrolling port waters

2.3. ***Perimeter Intrusion Detection*** -- Generally, it is a common practice to deploy security officers at stationary and roving posts along the perimeter. These posts may include: security officers positioned in elevated towers along the perimeter, walking along the perimeter barrier, and patrolling via mobile means. For maximum efficiency and effectiveness, a K-9 Patrol Team may be utilized to patrol the perimeter. Research by US law enforcement has determined that the deployment of K-9 Patrol Teams is a force-multiplier and one K-9 Team is as effective as the deploying of three individual police officers. Perimeter intrusion detection can also be accomplished by or enhanced thru the use of technological security systems; among them CCTV cameras, buried or taunt cable, microwave curtains, dual-technology PIR motion detectors, and laser beams, all which may be integrated into a manned central station.

Photo 15.3. – Perimeter Security Tower

2.4. ***Entrance & Exit Gates*** -- The number of port entrances and exits should be limited to a minimum and their purposes specifically defined. There should be separate gates for pedestrians and vehicles. Likewise, there should be separate gates for the entrance and exit of trucks transporting containers/cargo and those vehicles driven by employees, vendors, clients, and visitors. Physically, the gates should be constructed so as to meet the same minimum standards as the chainlink perimeter barrier. These gates should lock with heavy-duty padlocks and the keys controlled by security personnel. A security gatehouse should be located at each primary access point. The gate house should have the basic items required to accomplish the tasks, such as a fire extinguisher, first aid kit, flashlight, rain gear, vehicle and visitor gate logs, 24-hour chronological security logbook, personnel authorization roster, telephone, emergency telephone notification list, security post orders, and a copy of the Emergency Action Plan.

2.5. ***Access Control Policy & Procedures*** -- All access points (gates) into the port should be strictly controlled and there should be a comprehensive policy and specific written procedures which define the access of persons (employees, visitors, contractors, truck drivers, ship chandlers, etc.), vehicles (employee and visitor cars, trucks, etc.), and items (cargo, containers, trailers, ship's goods, spare parts, etc.) into and out of the port. "Authorized Personnel Only", "Identification Checkpoint" and "Subject to Search Upon Entry and Exit" signs should be posted and highly visible at all access points. Security officers posted at pedestrian gates should stop and challenge all persons, inspect their identification badges, and search any boxes, briefcases, or other items for contraband. Employees should present their ID badges to the security officer upon entrance and exit and wear their badges at all times while in the port. All visitors (clients, vendors, contractors, etc.) should be stopped at the gate, their visit confirmed with the sponsoring port employee, a temporary badge issued and visitor log completed, and any items opened and inspected for contraband. The interior and trunks of all vehicles should be visually checked for contraband. No privately-owned vehicles should be permitted inside the terminal. All trucks entering the cargo gates should be stopped, the driver's license checked for validity, the cab inspected for contraband and unauthorized persons, container seals inspected, and relevant information recorded on a comprehensive gate log.

Photo 15.4. – Vehicle inspection for contraband

Photo 15.5. – Gate inspection of license and interior of cab

2.6. ***Access Control Badge System*** -- Each person entering the port should be issued an identification badge. The ID badge program should be managed by a computer-based system which functions with proximity or magnetic strip badges, assigns zones of access, permits or denies a person's access into a specific zone, and records this activity into a data base. The front of the employee ID badge should have a color photo, the employee’s name and signature, government identity document or passport number, position, and an expiration date. The back of the ID card should note the employee’s date of birth, height, weight, color of hair and eyes, complexion, and the signature of the Port Director. Each employee’s badge should be programmed to allow access to specific zones, this being based on his/her job or position requirements. Employees who have forgotten or lost their badges should be issued a “temporary badge” for the day or while a new badge is being prepared. Visitor badges generally are for “one-day use”, disposable, and should note the name of the visitor, government identity document or passport number, area or zones visiting, and the date issued. Non-employees who temporarily or frequently work in the port - such as contractors, clients, and government representatives - should be issued a badge similar to the employee ID badge (but a different color). A permanent record of the issue all non-employee badges (with the captured data) should be maintained for at least two years.

2.7. ***Narcotics Control at Access Points*** -- Attempts to smuggle drugs through the access points and into the port may be conducted via hand-carried items, inside vehicles, and in containers/trailers and their cargo. While hand-carried items, such as briefcases, boxes, etc., can be effectively inspected by a “hand-search” by the Security Officer, it is not as practical (time wise) or effective to do so in the case of a loaded cargo container, empty trailer, or vehicle. In these cases, highly trained and certified Narcotics Detection K-9 Teams should be positioned at the access points and utilized to inspect the containers, cargo, and vehicles for narcotics. Alternatively, if financially possible, container X-ray stations should be positioned at the vehicle and container entrance points to screen for narcotics (as well as other contraband).

Photo 15.6. – Narcotics Detection K-9 Team at Cargo Gate

2.8. ***Explosives Detection at Access Points*** -- During times of heightened risks of terrorist attacks, bombing or violent labor conflicts, extra security measures should be implemented to screen for explosive devices and weapons entering the port. In the event that there is a specific threat or reliable information of a planned attack, the security procedures should be further enhanced. The four primary means of searching and screening for explosive devices and weapons are: a visual and hand-search, the use of a vapor analyzer to detect chemical odors from explosives, an X-ray machine (which vary in size from those used to screen letters/parcels to those that inspect vehicles and shipping containers), and an Explosives Detection K-9 Team. These four measures may be used independently or in combination; this generally being determined by the level and type of threat. Special attention should be given to suspicious mail and delivery packages and unattended vehicles positioned at access points or near key assets or buildings.

2.9. ***Weapons of Mass Destruction Detection at Access Points*** -- Ports must develop, test, and continually update contingency plans for the rapid deployment of systems and measures for the detection of chemical, biological, and nuclear weapons (typically referred to as Weapons of Mass Destruction). In many cases, the port will rely on the national government to provide such technical capabilities, however, it is critically important that the Port Security Director develop the policies, plans and procedures which will ensure a successful integration of these measures without significantly impacting the port's business or endangering the safety of its personnel. These contingency plans and procedures should be fully coordinated with the relevant government agencies and "tested" on a periodic basis. The contingency plans will interrelate with the port's "Disaster Preparedness and Recovery Plan" – which ensures business continuity and the safety and security of the personnel.

3. INNER SECURITY RING

3.1. ***Mobile Security Patrols*** -- The interior areas of the port, such as the container stacking zones, cargo staging areas, facility and maintenance buildings, equipment storage areas, and berths should be patrolled continuously by security officers in vehicles. These units should patrol in separate, overlapping zones. These security personnel should monitor general yard activities, restrict the movement of tractor-trailer drivers to within their vehicles, observe the transloading of cargo containers, and monitor the activities of stevedores and laborers working on the docks.

3.2. ***Foot Security Patrols*** -- The conducting of periodic inspections and Tallies of containers and seals throughout the yard by the security officers are effective deterrents to cargo pilferage, drug smuggling, and container manipulation, as well as a means of establishing a specific time period of an incident. The foot security officers should be constantly vigilant that personnel are wearing valid ID badges and are in their authorized zones, that doors and windows of all structures and buildings are secured during non-operational hours, and that drivers are not operating equipment at high rates of speed or in a dangerous manner.

3.3. ***Security Operations Command Center*** -- Security systems specialist (s) should be deployed 24 hours per day in the Security Operations Command Center for the purpose of observing and operating the central station system (which manages and controls all perimeter intrusion detection measures, CCTV deployed in the patio, on the berths and outside/inside buildings, building intrusion and panic alarms, access control system, fire alarm systems, etc.). All security systems should be fully integrated and support each other in the event of an incident.

3.4. ***Shift Security Supervisor*** -- There should be one person designated as the overall Shift Security Supervisor and he should direct, lead, and manage the terminal security officers and other deployed security resources (K-9 Teams, Security Operations Command Center personnel, Vessel Security Teams). The Shift Security Supervisor is a first-line management position and is a critical part of the overall security program. The Shift Supervisor should constantly patrol (in vehicle) the port, inspect/supervise security personnel, interact with other port managers, and respond to and take charge of incidents or potential security situations.

4. SITE & ASSET-SPECIFIC SECURITY RINGS

4.1. ***Administrative Office Building*** -- Dedicated resources should be deployed and procedures established to ensure the security of the building and its contents, and the safety of its occupants. The number of entrances and exits should be restricted to a minimum, with doors being secured with deadbolt locks when not in use. A security officer should be posted at each unlocked exterior-access door. Keys should be kept to a minimum and issued on a restricted basis by a designated Key Custodian. A computer-based key management system should be utilized. First-floor level windows (and those below) should be protected by bars or wire mesh. Lighting on the exterior of the building should be at the same level as that along the perimeter. At the main entrance, a security officer should screen all persons, check ID and visitor badges, and search all handbags, briefcases, boxes, etc. for weapons and contraband. A segregated reception area should be located inside the entrance. All visitors should be escorted into the interior offices by the sponsoring port representative. The interior of the building should be divided into functional zones in order to establish access zones for employees. Access into each zone should be regulated via the ID badge system. The main entrance, secondary access points, and the reception should be under constant surveillance by CCTV cameras, which are monitored/recorded by specialists in the Security Operations Command Center. Other sensitive areas, such as cashier windows, computer and telephone rooms, etc., should be under observation and security monitoring by intrusion alarms and CCTV cameras.

4.2. ***Bonded and High Risk Warehouses*** -- Security measures and procedures similar to those noted above (4.1.) should be implemented to ensure the security and integrity of the cargo, building, and personnel.

4.3. ***Critical Assets and Essential Equipment*** (Cranes, electric plants, telephone buildings, etc.) -- Security measures and procedures similar to those noted above (4.1.) should be implemented, as appropriate, ensuring the security and integrity of the equipment and assets.

5. VESSEL SECURITY RING

5.1. ***Basic Concept*** – Like other critical assets within the port, vessels must have their own security ring, which is a part of, but necessarily independent of, the terminal security apparatus. The key to effective vessel security and deterring/preventing incidents of stowaways, piracy, drug smuggling, pilferage, and terrorism is: exercise strict access control at the gangway -- to include a search of all items carried onboard, know who is onboard at all times, maintain a secured waterside, and conduct post-arrival and pre-departure inspections. All vessels calling on the port should be assigned a Vessel Security Team (VST). The VST should be deployed from the time of arrival until time of departure. Upon each arriving vessel's clearance by government officials, the VST should immediately board the vessel and conduct a quick inspection of the deck and exterior of the superstructure. This inspection is to detect stowaways, terrorists, or narcotics, unlocked doors into the superstructure, potential HAZMAT emergencies, etc. All discoveries of undocumented persons, suspected narcotics, or HAZMAT situations should be reported immediately to the Captain. Other security discrepancies should be noted in the gangway logbook and reported to the Chief Officer. Following this inspection the VST officers should deploy to their positions and continue with their duties.

5.2. ***VST Deployment for LO/LO Commercial Cargo/Container Vessel*** -- The Vessel Security Team should consist of no less than three Security Officers and one VST Supervisor:

5.2.1 One (1) Security Officer posted at the gangway to control and document the entrance and exit of persons (stevedores, crew, visitors, vessel agents, government officials, etc.) and search all parcels, bags, water coolers, etc. carried on and off the vessel.

Photo 15.7. – Inspecting/retaining port ID badge of stevedore

5.2.2. One (1) Security Officer patrolling the deck to monitor activities of the stevedores and ongoing cargo operations.

5.2.3. One (1) Security Officer patrolling the waterside, scanning the waters for ”swimmer” stowaways, scuba divers, drug smuggler launches, etc.

Photo 15.8. – Waterside Security Patrol during Threat Alert

5.2.4. One (1) VST Supervisor constantly patrolling the vessel decks and inspecting and supervising the operations of the security officers and taking charge of security situations. All empty containers not inspected by port Checkers should be inspected and sealed dockside at the hook by the VST Supervisor.

5.3. ***VST Deployment for RO/RO Vessels*** -- The Vessel Security Team should consist of no less than four Security Officers and one VST Supervisor:

5.3.1. One (1) Security Officer posted at the top of the Ramp to control and document the entrance and exit of persons (stevedores, crew, visitors, vessel agents, government officials, etc.) and search all parcels, bags, water coolers, etc. carried on and off the vessel. This officer should also constantly scan the dockside for unusual activity.

5.3.2. One (1) Security Officer posted on the ramp to inspect the undersides of trailers, inside vehicles and Ottawas, and search/seal empty containers for the presence of stowaways, narcotics, and terrorists.

Photo 15.9. – Inspection of interior of Ottawa entering vessel

5.3.3. One (1) Security Officer patrolling the internal deck where loading trailers/equipment are being staged.

5.3.4. One (1) Security Officer patrolling the weather/upper deck waterside, scanning the waters for ”swimmer” stowaways, scuba divers, drug smuggler launches, etc.

5.3.5. One (1) VST Supervisor constantly patrolling the vessel decks and inspecting and supervising the operations of the security officers and taking charge of security situations.

5.4. ***<u>Key Vessel Security Procedures</u>*** - Noted below are key procedures proven to yield positive results in maintaining effective vessel security.

5.4.1. Post a sign at the gangway which advises “Authorized Personnel Only – Present ID to Gangway Security – All bags, packages, etc. will be searched for weapons and contraband.”

5.4.2. All stevedores and visitors relinquish their port ID badges or national ID cards to gangway security officer while onboard.

5.4.3. Use Visitors Log, Stevedore List, Shorepass Log, and security logbook to document the entrance and exit of persons and all security incidents.

5.4.4. Maintain all Superstructure doors and cargo and deck hatches secured when not under guard.

5.4.5. Deck maintenance and storage lockers and crane access hatches should be kept secured when not in use.

5.4.6. Rat guards on mooring lines.

5.4.7. Secure anchor chain cover while in port .

5.4.8. Stevedores restricted to immediate work areas.

5.4.9. Jacobs ladder and Pilot ladder secured.

5.4.10. Cargo bay access hatches locked when not in use.

5.4.11. Waterside/Dockside illumination during night.

5.4.12. Use plastic/paper seals on access points of minimum usage.

5.4.13. Place sawdust or flour on deck around anchor chain and mooring lines holes and in key crawl spaces (entry noted by hand and footprints).

5.4.14. No POVs parked on dock next to vessel.

5.4.15. All ship's stores and ship chandler products searched by Narcotics Detection K-9 Team dockside.

5.4.16. All empty containers should be inspected for narcotics and stowaways and sealed prior to lading onboard the vessel. The container and seal numbers for all containers/trailers loaded onboard should be recorded on a Tally Sheet.

5.5. ***Pre-Departure Search for Contraband & Stowaways*** --

Upon completion of cargo operations, the VST Supervisor should coordinate and lead the officers (with the exception of the officer posted at the gangway) in a systematic and comprehensive search of the vessel for stowaways and narcotics. The gangway security officer should restrict access to the vessel during this inspection. Upon termination of the vessel search, the VST Supervisor should complete a "Vessel Search Certificate" and provide signed copies to the Captain, Vessel Agent, and the Shift Security Supervisor.

Photo 15.10. - The vessel inspection begins by checking each cargo bay

Photo 15.11. – This includes ventilation shafts and crawl spaces between bays

Photo 15.12. – Next, the security officers inspect the exterior of the Superstructure

Photo 15.13. – The VST then inspects the main deck -- from Stern to Bow

Photo 15.14. – Inspect the interior of fire hose boxes, storage areas, and cranes

Photo 15.15. – The vessel search is completed following an inspection of the interior of the Superstructure, from the rudder room to the Bridge

6. SECURITY PERSONNEL EMPLOYMENT & TRAINING –

While not a component of a specific security ring, proper pre-employment screening, training, and equipping of security personnel will directly impact on attaining the desired results of security personnel deployed in the various rings and the success of the overall port security program.

6.1. ***<u>Pre-Employment Screening</u>*** -- The screening of candidates for employment with the security department should follow the steps noted below:

6.1.1. Candidate completes a detailed employment application and provides "good health" certificate, "No Police Record" certificate, and copies of all education and training documents.

6.1.2. Candidate is interviewed by a security supervisor.

6.1.3. HR department verifies prior employment and references.

6.1.4. Internal Security Investigator conducts interviews of candidate's neighbors and prior employers and checks National Police records.

6.1.5. Candidate undergoes Drug Use Test.

6.1.6. Candidates for sensitive positions (K-9 Handler, Investigator, Supervisor, etc.) undergo polygraph.

6.1.7. Candidate receives final interview by Security Manager.

6.1.8. HR advises candidate of employment offer and candidate signs employment contract.

6.1.9. HR establishes a permanent personnel file, which includes the signed contract, completed application and photo, and all screening and investigation documentation.

6.2. ***Basic Security Training*** -- All new security personnel, regardless of their permanent assigned position, first should be fully trained in the basics of seaport security. A comprehensive course for new security personnel would be approximately 200 hours in duration and include as least the following topics:

6.2.1. Security Definitions in a Port Environment

6.2.2. Discipline, the Chain-Of-Command, and Ethics

6.2.3. Legal Considerations

6.2.4. Uniform & Equipment Presentation

6.2.5. Personal Defense Tactics

6.2.6. Use of the ASP or PR-24 Baton

6.2.7. Use of CS/CN Gas

6.2.8. Access Control Of Vehicles and Persons

6.2.9. Security Of Installations, Offices, and Warehouses

6.2.10. Vehicle and Foot Patrols and Static Posts

6.2.11. Report Writing

6.2.12. Security Forms and Documentation

6.2.13. General and Administrative Orders

6.2.14. Post Orders and Special Orders

6.2.15. Vessel Security Operations and Post Orders

6.2.16. Detection and Search Of Persons & Vehicles

6.2.17. Role of Internal Security & Intelligence Operations

6.2.18. Role of the Shift Security Supervisor, K-9 Units, and other Special Services

6.2.19. Leadership, Motivation, and Conflict Resolution

6.2.20. First Aid and Fire Fighting

6.2.21. Use of Radio and Communication Etiquette

6.2.22. The Business & Functioning of a Commercial Seaport

6.2.23. Usage and Qualification with issued Pistol and Shotgun

6.2.24. Theft and Cargo Pilferage

6.2.25. Narcotics Smuggling, Stowaway, and Piracy -- Trends and Techniques

6.2.26. Terrorism Awareness

6.2.27. Civil Disturbances, Protests, and Labor Strikes

6.2.28. Hazmat Recognition and Emergency Response

6.2.29. Bomb Threats and Search Procedures

6.2.30. Familiarization with the Port Security SOP Manual

6.2.31. Review of Port Emergency Action Plan

6.2.32. Port Threat Assessment

6.2.33. National & International Port Security Regulations

Photo 15.16. – Port Security Officer Training

Photo 15.17. – Students learning fire fighting techniques

Photo 15.18. – Executive Protection Team training

6.3 ***Security Officer Equipment*** -- All Security Officers and the Shift Security Supervisor should wear a police or military-style uniform, hat, and black military boots. Each should be issued a safety vest and helmet and wear a black nylon military equipment belt which holds a 3-D cell Maglite flashlight, 2 flexcuffs, ASP or PR-24 baton, radio, CS/CN gas, issued pistol, and extra ammo.

Photo 15.19. – Properly uniformed and equipped Security Officer

7. PORT SECURITY DIRECTOR - All World Class Seaport Security Programs require the assignment of a highly experienced, full time Security Director, and the support of a capable administrative staff. The Security Director should have a military and/or law enforcement background, extensive leadership and management skills, a solid understanding of the commercial maritime business and how a seaport functions, the ability to lead a large and multi-faceted security organization, and broad knowledge of and experience in assessing and successfully confronting the various security threats faced by a commercial seaport. The Security Director is charged with the development, implementation, leadership, and management of the overall Seaport Security program. In addition to managing all security operations and resources, the Security Director should define and establish all security policies, plans, and procedures -- to include the development of the Port Security SOP Manual, the Port Emergency Contingency Plan, and the Disaster Preparedness and Recovery Plan.

8. SECURITY SOP MANUAL and CONTINGENCY PLANNING -- There is an old military adage which states, “Proper Planning Prevents Poor Performance.” This is likewise true for Port Security. The absence of comprehensive, realistic, and tested written security policies, plans and procedures will ensure the failure of the Port Security Program. There are three manuals that are key to the successful design, implementation, and management of the security program. These are the Port Security SOP Manual, the Port Emergency Contingency Plan, and the Disaster Preparedness and Recovery Plan. A brief description of each is as follows:

8.1. The Security SOP Manual clearly and in detail defines the policies, plans, and procedures for all security-related activities, operations, functions, responsibilities, processes, and personnel. The breadth of issues addressed in the SOP Manual is extensive and ranges from Program Vision to Personnel Security Standards and Training to Physical Security Measures and Access Control Procedures to Computer Security and Competitive Espionage, and from Security Post Orders to Serious Incident Management.

8.2. The Port Emergency Contingency Plan identifies step-by-step procedures in response to various crisis situations, including assaults, assassinations, kidnapping, terrorist attacks, civil disturbances, labor unrest and strikes, HAZMAT incidents, fires, and natural disasters.

8.3. The Disaster Preparedness and Recovery Plan defines plans and procedures to ensure business continuity following natural and man-made disasters which significantly affect the port, such as an earthquake, tornado, hurricane, HAZMAT incident, and terrorist attack using WMD and other devices.

In order to meet the increasing and ever-changing security challenges and threats to seaports of the world, port management must design and implement a security strategy that is based on the concepts of “Defense-in-Depth” and “layered, inter-relational security rings.” A well-planned strategy, when combined with the leadership of a highly professional Security Director, deployment of a well-trained security force, and preparation of a comprehensive Security Standard Operating Procedures Manual and Emergency Contingency Plan, will ensure the success of the security program in deterring or denying current and anticipated security challenges and meriting recognition as a World Class Seaport Security Program.

The author is the co-founder of Phoenix Management Services Group in the USA and Panama and founder of Operations Support Services (OSS) -- USA and Costa Rica. Combined, these companies provide maritime and port security services to 15 of the world's largest Shipping Lines. Michael designed, implemented, and managed the internationally-acclaimed seaport security program at Manzanillo International Terminal – Panama, the largest container port in Latin America, and is credited with pioneering the Maritime Security Team (Anti-piracy/stowaway/drug trafficking) concept in commercial cargo shipping and currently has Teams positioned on vessels of four Shipping lines which transverse the Pacific and Atlantic Oceans and the Caribbean Sea. The author and his staff have trained hundreds of private security officers, Shipping Line personnel, and Customs/Military officials – from Chile to Mexico -- in Seaport/Vessel Security and Anti-Smuggling operations. Michael has over 14 years of progressive experience in US Law Enforcement, Military, and Intelligence organizations. A former US Army Commissioned Officer who served in Airborne Infantry, Military Police, and Military Intelligence units, the author completed undergraduate and graduate academics at the University of Baltimore. Michael held a Top Secret security clearance in the Central Intelligence Agency, where he specialized in counter-narcotics trafficking and international terrorism and served on the Vice President's Narcotics Interdiction Task Force. Mr. McNicholas has been a sole-source contractor for the US Defense Intelligence Agency on maritime security topics and has conducted various briefings to senior intelligence officers and analysts at the US Defense Intelligence Agency and Pentagon. The author currently serves as a Special Advisor to the Congress of Panama on counter-narcotics, terrorism, and intelligence issues. Michael has authored several training manuals and publications on seaport and maritime security, as well as various Intelligence Assessments, to include "The Reverted Panama Canal: Security Challenges and Defense Capabilities" and was contracted by Rand Corporation, under funding by the Defense Intelligence Agency, to publish an analysis of the origins and routes of arms procured by Colombian Guerrilla and Para-Military groups.