

management approach as used within the private sector. This GAO report explained how a company successfully created a security plan using a risk-based approach. Like the company described in the GAO report, the Coast Guard's approach to commercial maritime security featured the systematic development and consideration of potential scenarios of concern. The generation of scenarios ensured completeness of the risk-based method (GAO/NSIAD-98-74).

Principles of Risk Management

Risk management principles acknowledge that while risk generally cannot be eliminated, it can be reduced. Risk reduction is done by adjusting operations to reduce consequences, threats, or vulnerability of a security threat (consequences, threats and vulnerability will be discussed later in this document). Generally, it is easier to reduce vulnerabilities by adding security measures than to reduce consequences or threats (although reductions in all three are possible).

Risk assessments provide visibility into those elements of the risk equation that exert the greatest influence on risk. Those elements become the priorities in the risk management approach. The goal for maritime security is to ensure that if the level of threat increases, either the consequences or vulnerabilities decrease enough to offset that increase.

Process of Developing Maritime Security Risk Assessments

First, to look at risk from the port level, local experts in the area of commercial maritime safety and security met with a team of professional risk consultants. Together we developed the *Port Security Risk Assessment Tool* (PS-RAT). The PS-RAT was provided to local authorities to evaluate vessels, facilities and infrastructure within their areas of responsibility for a variety of threat scenarios. The approach used for the PS-RAT was as previously described and advocated by GAO, where risk was assessed in terms of threat, vulnerability and consequence. The PS-RAT was initially implemented Coast Guard wide on 16 November 2001 and the individual COTPs completed baseline risk assessments on vessels, facilities, and infrastructure within their area of responsibility. Nationwide, the local assessors evaluated nearly 5200 scenarios on more than 2000 unique assets and infrastructure elements.

Second, at the area level, regional Coast Guard and other maritime experts in the area of commercial maritime safety and security compiled and analyzed the local level PS-RAT results

to gain a better understanding of the security risks affecting their Coast Guard Districts and Areas. This assessment identified some recurring scenarios and common issues that needed to be addressed beyond the local level. It also helped clarify the need for another tool with a wider perspective that would be capable of evaluating risks at the national level.

Because of the local, relative nature of these assessments the PS-RAT did not support the national comparisons that were necessary for strategic planning. To accomplish strategic planning at the national level, a third team of Coast Guard subject matter and risk experts produced the *National Maritime Homeland Security Risk Assessment Tool*. Referred to in maritime circles as the *National Risk Assessment Tool* (N-RAT), the N-RAT provided a foundation for risk-based prioritization and subsequent regulatory assessment closely aligned with the guidance on conducting security risk assessments recommended by the GAO (GAO/NSIAD-98-74, GAO-02-150T, GAO-03-616T). The results of the N-RAT provided a national evaluation of the relative security risk facing the Marine Transportation System of the U.S. The experts compared the results from the national assessment with the previously performed local assessments (PS-RAT) to ensure that consistent assumptions were made and that comparable measures of risk were produced.

What Was Assessed

The Coast Guard used the N-RAT to determine risks associated with specific threat scenarios against various classes of targets within the Marine Transportation System. The targets considered included vessels, facilities, waterways, and marine-related transportation systems. This allowed the Coast Guard to systematically consider all segments of the commercial maritime community to evaluate their potential for being involved in a transportation security incident.

Maritime Security Incident Scenarios

The scenarios considered each element within the maritime community with respect to three general exposures: Susceptibility as a target; Use as a means of transferring or enabling the transfer of terrorists or terrorism-related materials; and Use of vessel or facility as a weapon.

The three above-mentioned general threat scenarios integrate multiple circumstances considered as specific attack modes. That is, there are subordinate scenarios under each general scenario. For example in the

basic threat scenario of "susceptibility as a target", a "boat loaded with explosives exploding alongside a docked tank vessel" is one attack mode while "tank vessel being commandeered and intentionally damaged" is another.

The N-RAT included over 50 target classes and 12 specific attack modes. This resulted in a matrix consisting of over 600 possible target/attack scenarios. Next, the 600 scenarios were screened for credibility by the expert panel. The credibility of a threat was based on the plausibility of an enemy actually carrying out the attack mode. For example, the "use as a means of transferring or enabling the transfer of terrorists or terrorism-related materials;" scenarios were screened out as "not credible attack modes" for military targets due to the inherent security measures in place. However, external attacks on these same targets were considered to be credible and were evaluated by the team. To balance comprehensiveness with efficiency, all scenarios were considered but only those scenarios deemed credible by the expert panel were further evaluated for risk.

Each credible threat scenario was evaluated by the panel of experts to determine the risk associated with a given attack against a specific target. The evaluation is based on a model showing the possible outcomes from any potential transfer or attack mode. Using previously cited GAO guidance in this area; the N-RAT risk was modeled as a function of the threat, vulnerability and consequences associated with each target/attack scenario. Each element is explained in the following sections. We realize that the terms used to identify each element may have recognized meanings in other contexts. In order to reduce confusion, we have included, as the first sentence in each element's discussion, the meaning associated with these terms for the purposes of the N-RAT.

Threat

The term "threat" is a measure of the likelihood of an attack. It represents the perceived probability of an attack based on maritime domain awareness and the existence of intelligence.

Within the N-RAT, five threat levels were identified. The threat magnitude was described, and scoring benchmarks were provided for each level. Each benchmark of threat intensity was assigned a probability of occurrence for use in risk calculations. For each scenario, the experts estimated the threat associated with an attack after considering the intent of hostile groups, prior security incidents, the capability