Information Paper
DoD TALON

The ability to acquire and analyze suspicious activity reports for indications of possible terrorist pre-attack activities is an absolutely critical component of the intelligence support to force protection mission. Terrorists have the advantage of choosing the time and venue for their attacks, but normally have to conduct extensive pre-attack preparations to maximize their chances of success. The pre-attack phase of a terrorist operation, however, is the period of greatest vulnerability to the terrorist group, since it must surface to collect intelligence and conduct physical surveillance and other activities of the target. If allowed to complete their attack preparations unhindered and proceed to the attack initiation phase undetected, they are almost assured of conducting a successful attack. Therefore, an effective system for detecting terrorist pre-attack activities is a high priority task for the intelligence community, law enforcement, security elements, and local community authorities.

The history of terrorism is full of instances where terrorist pre-attack surveillance and other activities either went undetected or unreported and was recognized only in hindsight. Two specific examples include the 1979 attempted assassination of the Supreme Allied Commander Europe and the 1996 attack on Khobar Towers in Saudi Arabia, which killed 19 U.S. airmen.

Recognizing these facts, shortly after 9/11, an ad hoc group of intelligence and security professionals, under the sponsorship of the Joint Staff, met to develop a system specifically designed to provide the capability to assemble, process and analyze suspicious activity reports to identify possible terrorist pre-attack activities. Since the US Air Force had already developed the Threat and Local Observation Notice (TALON) reporting system, it was immediately adopted for DoD wide use.

To further develop the program, in May 2003, the Deputy Secretary of Defense established the TALON reporting format as the formal mechanism for assembling and sharing non-validated domestic threat information among intelligence, counterintelligence, law enforcement, security, and force protection entities. The TALON is designed to capture non-validated threat information and security anomalies indicative of possible terrorist pre-attack activity.

The TALON reporting requirement applies to all DoD elements with a force protection mission, to include law enforcement, security, intelligence and counterintelligence elements. Reportable events include non-specific threats to DoD interests; suspected surveillance of DoD facilities and personnel; elicitation; tests of security; unusual repetitive activity; bomb threats; any other suspicious activity. The TALON report is a simple web based entry form.

In support of NORTHCOM, CIFA analyzes TALON reports with a DoD nexus in the U.S. for force protection, critical infrastructure protection and Foreign Intelligence Security Service information. CIFA creates a variety of finished products to include: Significant Activity Summaries, Special Reports, Briefings, and Threat Advisories.

CIFA has established a Standard Operating Procedure (SOP) for TALON reports to ensure they meet intelligence oversight requirements and that U.S. person information is collected and retained only as authorized by Executive Order 12333. TALON reports are collected, retained, and disseminated in compliance with the regulations that limit DoD handling of information about U.S. persons and non-DoD civilians.