Army Regulation (AR) 381-12, Threat Awareness and Reporting Program (TARP) and the supporting training materials were developed to resolve a finding from the Army's initial review (Nov 2009 - Mar 2010) of force protection procedures following the Fort Hood shooting incident. The finding concluded TARP's predecessor - Subversion and Espionage Directed against the US Army (SAEDA) - was too narrowly focused on Cold War era threats, lacked centralized program management and oversight, and would be more effective with standardized training content. TARP training is now centrally funded and managed by HQDA, Office of Deputy Chief of Staff, G-2. The training includes a web-based module to support distance learning and an interactive module to support live training by Army CI special agents.

The Army combats insider threats with a holistic approach that leverages counterintelligence, personnel security, law enforcement, and information assurance capabilities. The Army developed a comprehensive strategy to synchronize disparate programs and elements involved in combating insider threats based upon recommendations from the review of the 2009 Fort Hood attack. The Army is institutionalizing Army Security Resiliency as a component of the Army Protection Program. The fiscal year 2012 National Defense Authorization Act, and the National Insider Threat Executive Order 13587 signed in November 2012, provide impetus for the Security Resiliency program's cross-discipline initiatives to provide the Army the earliest possible opportunity to identify and evaluate behavior that could indicate a need to take action to prevent an incident. Security Resiliency improves the Army's personnel security, information sharing, network auditing, force protection and engagement with the Federal Bureau of Investigation. The outcomes counter insider threats, improve risk management, and promote overall mission assurance.

Lawrenc D. Gillis 6/27/13 8:18 AM
Deleted:

---

1. Have other defense/non-defense agencies asked the Army for guidance on its program? If so, what agencies and what advice has the Army given them?

ANSWER: Army's Threat Awareness and Reporting Program (TARP) implements guidance in Department of Defense Directive (DoDD) 5240.06, Counterintelligence (CI) Awareness and Reporting. AR 381-12 is unclassified and available to any individual or federal agency. Army has not provided guidance to other federal agencies; however Army did provide the Navy, Air Force, Defense Intelligence Agency, and the Joint CI Training Academy information on the content and scope of TARP training materials.

2. What's the current annual budget of the program and what was the annual budget for the Subversion and Espionage Program the year before it became the insider threat program?

ANSWER: From approximately 1963 to 2010, SAEDA was a mandatory annual training requirement for all Army personnel. During this period, Army assigned execution of the SAEDA program to CI elements integrated into the force structure and these elements accomplished the training using unit resources and locally-produced training materials. Prior to fiscal year (FY) 2011 Army did not centrally fund or manage SAEDA and expenditures were not tracked as a specific CI project. As previously stated, TARP is now centrally funded and managed by HQDA, Office of

Deputy Chief of Staff, G-2. In FY 13 Army allocated $1.4 million to execute TARP.

3. How does the Army measure success of the program? Through metrics? How many insider threat cases were opened during the last available calendar or fiscal year? During that same year, how many have been prosecuted and separately how many led to administrative actions? How many were dropped? And how many are still pending?

ANSWER: TARP is mandatory training and our basic measure of success is whether 100% of Army personnel received the training. We collect training data quarterly from CI elements worldwide. We also collect lessons learned and best practices from CI agents in the field. We use this information to revise the training annually. Because TARP is a continuation of a program more than 50 years old, we have not seen a significant spike in reporting which can be wholly attributed to TARP; however, from FYs 11 to 12, Army has experienced about a 30% increase in terrorism-related reporting. TARP reports do not always result in a formal CI investigation. All initial TARP reports are reviewed to determine the nature and validity of the allegation. In cases where there are no indicators of foreign intelligence or international terrorism involvement, or indicators of extremist activity that may pose a threat to the military operations, the report is typically referred to local security managers, the chain of command, the personnel security adjudication facility, or law enforcement.

4. How did the Army come up with its program - did it look to certain research? If so, what? If not, what did it look to craft the program?

ANSWER: As previously stated TARP is not a new program. In 2010 Army changed the title of Army Regulation (AR) 381-12 from SAEDA to TARP. The purpose of the change was to communicate that threats to the Army were not limited to subversion and espionage. As for the content of the program, both the AR and the supporting training materials were updated and revised to include indicators of international terrorist-associated insider threats or extremist activity that may pose a threat to the military operations.

5. AR 381-12 identifies not just classified information, but sensitive information, as needing protection from the insider threat. Have there been any security violation cases involving sensitive information since this program was launched?

ANSWER: The focus of AR 381-12 is to ensure Army personnel understand and report foreign intelligence and international terrorist threats. It is not the Army’s primary guidance for recognizing, reporting, or handling security violations. Sensitive information is data which has not been specifically authorized to be classified. Sensitive but unclassified information, if compromised or disclosed to individuals without a need to know, could adversely impact the conduct of Army missions or the privacy of individuals. Sensitive information takes many forms within the Army. It could relate to counter-improvised explosive device techniques; military convoy procedures; personnel privacy information; personal medical information; military deployments; and information relating to communications or weapon systems. Allegations Army personnel mishandled sensitive information are not reported or handled as security violations.

Security violations only apply to classified information. For example, when an Army unit is alerted for deployment, while information on the destination, deployment date, and general mission are typically unclassified, members of the unit are instructed not to provide specific details to the public.

6. Has the Army seen an uptick in the number of security violations reported by co-workers as a result of this program? If so, by how much (percentage or hard numbers)?

ANSWER: As noted above the Army does not classify mishandling of sensitive information as a security violation. Mishandling sensitive information would typically be handled in accordance with established procedures for commander's inquiries or employee misconduct. In FY 12, Army CI received 822 CI Incident Reports (CIR) which lead to nine full-field investigations and 75 preliminary inquiries. So far in FY 13 Army has received 736 CIRs which lead to six full-field investigations and 70 preliminary inquiries.

7. Are there any cases that highlight the success of the program that have been made public because of an arrest and/or prosecution (perhaps in the UCMJ system)?

ANSWER: The Army CI investigations of MAJ Seiverak Inson and Army Pfc. Naser Jason Abdo were initiated based on CIRs from Army personnel. A military jury convicted Army Major Seivirak Inson of unauthorized possession of classified documents and giving a document with classified assessments of Cambodia to a person not entitled to have it. The jury sentenced MAJ Seivirak Inson to ten years confinement. Army Pfc. Naser Jason Abdo was convicted of collecting bomb-making materials for an attack on a Texas restaurant full of Fort Hood troops. A federal jury convicted Abdo on six charges, including attempting to use a weapon of mass destruction.