
When Things Go Wrong: The Role of the Defense Criminal Investigative Service in Foreign Military Sales

By

**Kevin O'Leary and Michael V. Fewell
Defense Criminal Investigative Service**

Introduction

The Security Assistance Program (SAP) has operated for many years making defense items and services available to allied and friendly governments all over the world. The program has been a tremendous success. With annual orders of about \$9 billion from over 130 countries, the security assistance program is a key tool in establishing security relations between the U.S. and many countries throughout the world. Since yearly deliveries of material and services are running around \$13 billion, there are obviously many satisfied countries that willingly participate in our security assistance efforts.

But what happens to the program when the buying country receives defective items in lieu of the items actually desired and needed? What happens when funds intended for badly needed and costly defense items and services are diverted to individuals for their personal benefit? Never happens, you say? Let's examine the level of threat these activities represent and how the Defense Criminal Investigative Service (DCIS) is structured and trained to assist the Security Assistance community. To do so, we will look at some investigations conducted by DCIS into various elements of the SAP and their results. In addition, we will discuss what assistance SAP personnel can provide during an investigation and look at current DCIS initiatives that will impact the SAP and Department of Defense as a whole.

DCIS and Fraud

DCIS, the investigative arm of the Office of the Inspector General for the Department of Defense (DoD), was established by Congress in 1981 to investigate and prosecute fraud involving DoD funds, people and programs. DCIS operates with funds appropriated by Congress as part of the DoD budget, and the Defense Security Cooperation Agency (DSCA) is one of many DoD components to which DCIS provides investigative assistance in matters involving fraud.

Fraud is generally defined as a lie concerning a material issue relied upon by the victim to his detriment and to the benefit of the liar. In a business transaction the lie is typically of such a magnitude that, if the victim knew the truth, he would not conclude the deal. In our context, the lie may concern the quality of product or service to be delivered, or the liar's intention to comply with contractual or regulatory provisions. Fraud also includes corruption--bribes paid to gain favor for the payer and recipient at the expense of unsuspecting parties, whether the foreign government or programs and individuals working in the SAP. When we speak of the SAP in this article, we include not only officials of participating governments, but also those individuals in the public or private sector who provide defense items and services.

Defective Products

DCIS investigation of fraud in the SAP began just a few years after the formation of DCIS. One of the first successful cases centered around a product substitution scheme in which there were two victims, the United States and the foreign government. Between 1985 and 1987, a U.S. contractor was awarded a series of Foreign Military Sales (FMS) contracts, funded under what was then referred to as the FMS Credit Program, to supply parts for trucks for the foreign government. The U.S. contractor agreed to the terms of the contract, which called for the products and services to be of U.S. origin. The contractor instead conspired with several U.S. vendors to obtain parts of lesser quality from countries other than the U.S. The identifying markings on the parts were removed, and the parts were repackaged and relabeled for shipment to the buying country. During the course of the investigation, it was revealed by the buying country's embassy in Washington that the foreign army had experienced major problems with the material in question, and testing of the parts by the U.S. Tank and Automotive Command (TACOM) disclosed that the parts did not meet specifications. The contractor and its president were fined over \$80,000, and the president was given six months probation. In cases such as these, the product sometimes has to be re-procured, creating a delay for the receiving country.

Theft

Another case where the victims were the United States and the foreign government involved a transportation scheme in which two U.S. contractors submitted fraudulent inland transportation invoices. The prime contractor, a freight forwarder, was awarded a Direct Commercial Sale (DCS) contract, financed under the Foreign Military Financing Program (FMFP), to provide freight forwarding services relative to the transportation of cargo from the U.S. to the host country port. The subcontractor was required to provide freight brokerage services to the prime contractor. Certain managers at the prime contractor conspired with the subcontractor to submit fraudulent invoices. The scheme was carried out through the establishment of "shell companies." The shell companies were represented as legitimate trucking companies responsible for transporting the cargo. The trucking companies did not have telephone listings, Dunn & Bradstreet reports, or possess valid Interstate Commerce Commission licenses. Invoices bearing the names of these companies for deliveries that were not actually made were submitted to the foreign country program office, and ultimately to the U.S. government, for payment. In other cases, legitimate invoices for actual deliveries by legitimate companies were inflated by several hundred percent. These invoices were also paid. The proceeds from these transactions were laundered through several domestic and foreign accounts controlled by the managers. The prime contractor agreed to pay the U.S. government \$1.25 million to settle potential civil false claims liability. The subcontractor was sentenced to over five years in prison and ordered to repay the government over a \$1,000,000.

Other schemes may not involve a U.S. victim or offender. The Country of Bandaria regularly deposited its own funds into its holding accounts administered by the Defense Finance and Accounting Service (DFAS) in Denver, Colorado to be used to purchase military equipment in the United States. A Bandarian Foreign Liaison Officer (FLO) acted as fiduciary for these funds. Acting in concert with others in the Bandarian military, the FLO directed transfer of several million dollars from the holding accounts to the Bandarian Air Force accounts that he controlled and used for legitimate purposes. From there, the FLO diverted funds to personal bank accounts, located in the U.S., of the FLO and other high ranking Bandarian officials. Simultaneously, forged Bandarian Letters of Offer and Acceptance (LOAs) came to the attention of DCSA,

suggesting that within Bandaria, the transfer of public funds to private accounts was being concealed with forged LOAs. Responsible Bandarian officials were placed under house arrest in Bandaria and tried there by court-martial.

False Certification

A European-owned U.S.-based company entered into an FMFP contract with a Middle Eastern country for the delivery of training aircraft. The European parent had to certify to the U.S. about non-U.S. content of the aircraft, thereby establishing a basis for U.S. funding of the contract. The certification to DSCA reflected that \$2 million of the contract price would fund non-U.S. components, with the remaining \$6 million to be U.S. content. However, the investigation by DCIS disclosed that the contractor could only support costs of approximately \$350,000 for alleged U.S. content. Prosecutors and investigators had to overcome several obstacles because of the corporate structure of the company. Key records were maintained overseas, and the corporation also reassigned key high level employees outside of the U.S. Despite these factors, the contractor was ordered to pay the United States over \$17 million for False Claim Act violations.

Bribery

Probably the most common issue in SAP investigations is that of bribery. In an effort to combat this problem, Congress enacted the Foreign Corrupt Practices Act (FCPA) in 1977 to curb abusive practices by some U.S. companies. To prove this offense, the Government must establish that something of value was offered by an individual or company to an official of a foreign government to unduly influence that official. The following examples illustrate the point.

A buying country had entered into a contract, funded with FMS loans, with a U.S. contractor to upgrade the foreign country's C-130 military transport aircraft. When this contract was signed, the contractor was required to submit signed certifications to the U.S. government. The signatory represented, among other things, that commissions would be paid only to bona fide employees or agencies which neither exerted or proposed to exert improper influences to solicit or obtain the contract as defined in the Federal Acquisition Regulation. The investigation determined that the U.S. contractor, in order to secure and maintain business with the foreign government, paid bribes amounting to over \$100,000 to foreign officials exerting influence on the C-130 program. The bribes were made through false sales representatives. Recipients of the bribes were an embassy employee and the buying country's air force chief maintenance officer. The contractor, as part of the plea agreement, paid over a million dollars in fines and penalties to the U.S. government.

In another case, the defense items were jet engines and related support equipment for F-16 aircraft, obtained on a Direct Commercial Sale (DCS), and funded via the FMFP. In 1984, a middle grade officer in the buying country's air force had conspired with a major defense contractor to, among other things, award subcontracts for engine support work in-country to a friend and business partner of the officer. Though invoices and milestone certifications attested to the completion of contract line items, reality was, in many instances, far different. For instance, one line item, priced at \$7 million, was never produced, invoicing documentation to the contrary. In addition, the price of the engines themselves had been inflated, ostensibly to cover the cost of flight tests, but in fact to generate proceeds to deposit in off-shore bank accounts belonging to the officer, the contractor's sales manager and a third facilitating party. In this instance, allegations of impropriety by the mid-level officer had surfaced in the buying country. As a result, a high level commission had been formed by the foreign government to look into the activities of this officer.

Although the allegations were dismissed, a second investigation was soon launched. This time, information surfaced that key conspirators had diverted funds to Swiss bank accounts. Interestingly, widely publicized accounts of the investigative commission did not result in any notification to U.S. authorities. It was not until several weeks after the arrest of the officer, following involvement of the local police, that the U.S. government became aware of the diversion of funds. Ultimately, the officer, now a brigadier general, implicated other officers and U.S. defense contractors. A common factor in the schemes was the diversion of security assistance funds for the personal gain of the officer and his co-conspirators or for projects that would not have qualified for security assistance funding. The investigation led to several different plea agreements and civil settlements, with recoveries to the U.S. Treasury and SAP of nearly \$100,000,000, much of which was returned to the foreign country trust fund account for future defense needs.

In another case, a major defense contractor entered into a commercial sale funded with FMFP funds, in which the contractor agreed to pay \$1.8 million to a foreign consultant, who also was a member of the buying country's parliament. In late 1989, a high ranking DSCA official observed from documentation from the Department of State Office of Munitions Control that the contractor was going to pay a commission associated with the contract. The official, having remembered that the DSCA certificate submitted by the contractor had reflected no commission or contingent fees were to be paid, notified both the contractor and the foreign government of the discrepancy. While the contractor insisted no commission had been built into the contract price, a later audit by the Defense Contract Audit Agency (DCAA) disclosed the improper payment. Corporate records obtained by means of a subpoena confirmed that the defense contractor had paid a foreign official for his influence. The contractor pled guilty to violating the FCPA.

A scheme that primarily involved the funds of the buying country, but was nonetheless prosecuted as an abuse of the SAP, involved the subversion of the Defense Reutilization and Marketing Service (DRMS) program. In this case, a FLO assigned to a U.S. Air Force base was authorized to make purchases of military equipment on behalf of the foreign country air force. Pursuant to a LOA, the foreign country was to receive equipment originally supplied by the DRMO and refurbished by a U.S. company. The transactions started out legitimately, but took on a different tone when the FLO, acting in his own personal interests, threatened the U.S. company responsible for refurbishing the equipment denial of further business unless the vendor paid him cash from these transactions. Also implicated in this scheme was a USAF country manager, who accepted approximately \$99,000 for his role in assisting the FLO. The country manager helped locate the equipment and had ownership of stock in the U.S. company that refurbished the equipment. The U.S. company and its officials and the USAF country manager pled guilty to their role in the scheme. The foreign country military and legal officials are pursuing prosecution of the FLO, who had received over \$240,000 as a result of these transactions.

In other cases however, where the contract only involved foreign funds, investigations have been discontinued in those instances in which the buying country was not interested in pursuing the matter. Although there may be complicity on the part of the defense contractor, because the primary victim in these cases is the foreign country itself and the perpetrators are based in the foreign country, there is little incentive to furnish documents or make witnesses available to the U.S. government.

The Investigation

If an investigation involving the SAP is initiated, there are several things you can expect as DCIS determines whether or not a crime or civil cause of action has occurred. Conducting investigations is a matter of, first, interviewing witnesses. Because you are the expert, investigators need to get an understanding of a particular contract and the program affected. Fraud investigations are paper intensive and investigations into security assistance matters are no exception. You might also be required to testify in a court proceeding, prior to which you will be briefed on procedures and instructed to simply answer the questions and tell the truth. Typically, the charges against those who perpetrated the fraud in the SAP have included submitting false claims to the U.S. government; making false statements to the U.S. government; conspiracy; money laundering and violations of the FCPA. Frequently, DCIS and other government agencies work with authorities in the buying country to complete an investigation.

These type of investigations have provided unique opportunities for the investigator, the prosecutor, and security assistance community as a whole. Issues involving sovereignty, court proceedings and collection of documents not seen in the typical investigations are dealt with in SA investigations. In one case, the foreign government cooperated by agreeing to allow the U.S. government to conduct depositions, pursuant to the Mutual Legal Assistance Treaty (MLAT) and other guidelines, in that country's court proceeding. In cases when that was not feasible (such as when national security concerns exist), agents and attorneys have conducted interviews outside the courtroom. Extraditions have been made in cases where there is no formal extradition process. In one case, a foreign country on the list of hostile/terrorist states agreed to prosecute a U.S. fugitive in their court, thus leading to the voluntary return of the fugitive to be tried in the U.S. Bank records, pursuant to the MLAT have been obtained from banking institutions located in European countries.

Current Initiatives

Beginning this year, an FMS block of instruction was added to the DCIS Special Agent Basic Training Course to discuss the unique aspects of security assistance investigations. Included in this block of instruction is material covered by students attending DISAM courses. The intent of this block is to familiarize agents with the SAP, and provide accurate and current information concerning the SAP. Other areas receiving more attention include technology transfer, electronic commerce and computer intrusions. Concerning technology transfer, there is more of a concern that individuals are diverting equipment from the intended or actual recipient to unauthorized countries. With the advent of electronic signatures and paperless contracting, DCIS is working with other agencies, such as the Department of Justice, DCAA and the DFAS to determine what impact the paperless initiative will have on the traditional methods of collecting documentary evidence. With the increase in "electronic business", there are and will continue to be new opportunities for the procurement and financial process to be manipulated. DCIS has also been tasked by the Secretary of Defense to include as one of their top priorities the investigation of computer intrusions. This effort includes working with other military criminal investigative organizations, such as the Air Force Office of Special Investigations, Naval Criminal Investigative Service and U.S. Army Criminal Investigation Command and foreign law enforcement organizations to tackle with what is becoming a global concern. It also includes taking proactive steps to meet with those agencies, such as DSCA, that are integrating and upgrading their information technology infrastructure (i.e., Defense Security Assistance Management System (DSAMS)), and offer our assistance in responding to intrusions that may

lead to anything from destruction of data to the theft of funds and sensitive procurement information.

What You Can Do

The security assistance community has brought to the investigator and prosecutor their expertise and insight to programs that have led to successful resolutions of significant investigations involving the subversion of the SAP. Ultimately, such cases, notwithstanding a few exceptions, may lead to a recovery of funds by the U.S. treasury or the foreign country trust fund account, and provide reassurance that the U.S. government will assist foreign countries when they have been defrauded. When you receive information that indicates the SAP may have been subverted, feel free to contact DCIS directly, or indirectly, through the DoD IG Defense Hotline (1-800-424-9098), which takes anonymous complaints. The DoD IG web page address is www.dodig.osd.mil.

Conclusion

There is no question that the overwhelming majority of people involved in the security assistance program, including those in the defense contractor community, are honest, talented and dedicated in their efforts to fulfill the mission of making available defense items and services to allied and friendly governments. The authors know this first hand from having worked with professionals of the DSCA and others involved in the security assistance community. While cases such as those described above bring a lot of publicity to the security assistance community, we believe that such cases are not the norm. However, the cases in this article are cited to illustrate that problems do occur and you are in the best position to help determine if that problem may be indicative of fraudulent activity. That such frauds may occur infrequently will be of no consolation if your program is the one subverted. Although neither you nor DCIS has any control over media coverage and congressional reaction to such cases, DCIS does have control over what we bring to the table. And what we provide is the expertise to respond to the fraud.

About the Authors

Special Agent Michael V. Fewell, an eighteen-year veteran with the Defense Criminal Investigative Service, is assigned to the Dayton Resident Agency. Agent Fewell began his government career with the Naval Security Group, after which he continued his Navy affiliation as a Reservist, concluding his career in 1997 with the rank of Commander. Following active duty with the Navy, Agent Fewell joined the Defense Investigative Service before moving to DCIS. He is a graduate of Indiana University. He can be reached at (937) 534-0100 or via email at Mfewell@dodig.osd.mil.

Special Agent Kevin O'Leary is a ten-year veteran with DCIS and is also assigned to the Dayton Resident Agency. Agent O'Leary began his government career with the U.S. Army Military Police Corps, and concluded his tour as a Special Agent with U.S. Army Criminal Investigation Command. He is a graduate of Wayland Baptist University. He can be reached at (937) 534-0100 or via email at Koleary@dodig.osd.mil.