

Customer: 516th Signal Brigade, U.S. Army

Location: Ft Shafter, Hi

Job Function: Installation and Implementation of Network Security Product (ISS Real Secure)

Contract Value: \$9,450,000 +

Contract Period: June, 1997 to Present

Overview:

According to Colonel Strong, the 516th Signal Brigade commander, "Penetration of our internet will be the cause of World War III." The US Army had a serious concern with the security of their networks. Each command implemented different plans in addressing this serious problem. As a result, in June 1998, the 516th Signal Brigade awarded SMF a contract to provide network security assistance.

After evaluation of the US Army's network system, SMF installed and implemented **ISS Real Secure**, a network security product. The first day after it was installed, there were 1500 attempted intrusions detected. A high percentage of the attempted intrusions came from repeated violators. Thus proving the effectiveness of ISS Real Secure, violators were now frustrated by their lack of success.

Dave Millard, the TNOSC chief, utilized the SMF contract to develop similar applications that involve technology services and contract avenues. SMF began with the initial team to implement the network security product and now have over 30 full-time personnel directly supporting the TNOSC, which perform the following functions.

- Software engineering and design- Using Oracle, Ada Programming Support Environments
- Testing hardware and Firmware
- Network Troubleshooting
- Data Collection

They are structured into response teams that include a high-level help-desk for the Theater, which is, manned 24 hours/day, 7 days/week. A network team and systems team complements them. In addition, the network monitoring team is comprised of programmers who collect data on the network and do trends/analysis.

Currently, the TNOSC experiences approximately 800,000 intrusion attempts a month. The SMF team identifies and investigates these intrusions. The TNOSC has a high concentration of Top Secret and Secret cleared SMF personnel.

Recently, the TNOSC underwent an evaluation by the US Army, where over 2500 servers were tested throughout the evaluation, identifying them as a model for the Army. As a result of the 516th network security proof of concept, the US Army has rolled out a similar team structure to Europe and Korea. PACRIM. They identified only 2 problems, which were immediately solved. They passed this

The SMF capabilities and flexibility have led to more opportunities. They are now looking to SMF to staff Network Security training for the PACRIM. Currently, the only US Army option is at Ft. Gordon, GA. In addition, they are considering adding analysts at sites throughout the field who will be able to implement plans/procedures as defined by the TNOSC team.