C. (U) FOREIGN INTELLIGENCE SERVICE (FIS) THREAT:

1. (S//NF) Multiple intelligence services maintain a presence within CONUS. China, India, Russia, Pakistan and France have been cited as the most aggressive, particularly with a focus on naval platforms. Intelligence collection efforts are constant and include targeting of traditional military assets, such as U.S. military plans, programs, disposition, readiness, capabilities, deployment preparations, and operations, as well as critical technologies and information systems. China, Russia, and Cuba pose the most significant FIS threats to DoN assets in Jacksonville. Jacksonville's proximity to Interstate 10 and 95 make it an opportunity target for foreign intelligence officers (IOs) en route to Miami and other vacation spots throughout Florida. Attempts to glean information about key DON technologies and deployments in Jacksonville through open-source Internet sites, email, and personal solicitation are expected to continue.

2. (S//NF) China primarily targets DoD contractors, U.S. military personnel, Chinese-Americans, defense-related industry, and dual-use technology programs. China employs a variety of collection methods, including unsolicited e-mail contacts, academic delegations, foreign exchange programs, indirect collection through third-country businesses and academic institutions, and collection from USN websites. China also uses the following state-owned organizations as collectors: The Chinese Academy of Science, the Chinese Association of Science and Technology, and a variety of front companies.

3. (S/NF) Despite warming relations with the U.S., Russia continues to target U.S. nuclear technology as a high collection priority. Both the Russian General Staff Main Intelligence Directorate (GRU) and the Russian Foreign Intelligence Service (SVR) target U.S. military installations, nuclear research facilities, academic institutions, and professional conventions. Russian collectors also use Internet and e-mail methods. Russian IOs and Diplomats routinely transit Florida, via I-95, en route to vacation sights, or Jacksonville International Airport (JIA) as part of Strategic Arms Reduction Treaty (START) inspection teams in Kings Bay, GA. During the period of 04MAY through 19JUN04, Russian Senior Consul and Suspected Intelligence Officer (SIO) Igor Y. Kochetkov drove round trip from San Francisco to Florida. The Travel Alert listed no stated purpose for this trip. Of note, KOCHETKOV departed San Francisco and made overnight stops in Los Angeles and San Diego before proceeding to Las Vegas. His reason for taking this circuitous route to Florida from San Francisco remains unknown.

4. (S//NF) French collection methods are diverse and aggressive. French intelligence recruits science and engineering students, uses foreign liaison billets within DoD commands, purchases U.S. firms to gain access to classified data, strongly requests information during hosted visits, exploits Internet websites and e-mail, and acquires technology with U.S.-based businesses.

5. (S//NF) India has attempted collection against U.S. nuclear submarine and naval technologies. India prefers anonymous collection methods like unsolicited e-mail requests and collection from USN websites.

6. (S//NF) Cuba views the U.S. as a major threat and has postured military and intelligence assets to counter the U.S. threat, placing a high priority on collecting information regarding U.S. military order of battle, indications and warning (I&W) and science and technology (S&T) information. Cuba effectively employs a wide variety of collection techniques that involve a combination of methods, including signal intelligence (SIGINT) and human intelligence (HUMINT). Cuba has enhanced its ability to intercept and exploit U.S. and hemispheric commercial and military satellite communications. Imagery has revealed that nine additional satellite dish antennas, which will likely collect against U.S. assets, were installed at a SIGINT facility near Havana. In 2004, Cuba acquired and fielded new cellular telephone intercept equipment obtained from a Panamanian company, targeting phones purchased on Cuba, as well as off-island.

7. (S//NF) The threat of collection by foreign contract employees is of concern. Representatives of countries constituting a collection threat to U.S. technologies maintain professional relationships with DON personnel. Trained intelligence officers, as well as co-opted foreign scientists, engineers, and academics are currently engaged in a large overt collection effort targeting U.S. technologies. These efforts, although less intrusive than clandestine collection efforts, are much more widespread and are generally accomplished through legal means.