COMMITTEES:
ARMED SERVICES
SUBCOMMITTEE ON READINESS
SUBCOMMITTEE ON SEAPOWER AND EXPEDITIONARY FORCES

JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY – RANKING MEMBER
SUBCOMMITTEE ON IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW

J. Randy Forbes
United States Congress
4th District, Virginia

307 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6365

425-H SOUTH MAIN STREET
EMPORIA, VA 23847
(434) 634-5575

2903 BOULEVARD, SUITE B
COLONIAL HEIGHTS, VA 23834
(804) 526-4969

505 INDEPENDENCE PARKWAY
LAKE CENTER II—SUITE 104
CHESAPEAKE, VA 23320
(757) 382-0080

October 2, 2007

The Honorable Robert C. Scott
Chairman, Subcommittee on Crime,
Terrorism and Homeland Security
B-370 Rayburn House Office Building
Washington, D.C. 20515

Bobby

Dear Chairman Scott:

As we have previously discussed, the issue of espionage and cyber-crime as it relates to China's influence and operations in the United States is of great concern to me. I am requesting that you schedule an oversight hearing of the Subcommittee on Crime, Terrorism and Homeland Security to investigate the extent to which Chinese espionage and cyber-attacks threaten the security of the United States and what legislation may be useful to aid law enforcement activities in this area.

Chinese military doctrine considers computer network operations as a force multiplier in the event of a confrontation with the United States or any other potential adversary. We know that Chinese cyber-warfare units are attacking computer systems in the United States today. In 2006, there were several attacks on U.S. government sites traced back to the People's Republic of China. Most recently, the Department of Defense confirmed a cyber-attack on the offices of Defense Secretary Robert Gates in June of this year.

The Attorney General has testified before this Committee that China represents the number one espionage threat to the United States. It is estimated that there are between 2,000-3,000 Chinese front companies operating in the U.S. to gather secret or proprietary information. Foreign intelligence operations gather sensitive information through legal and illegal means, such as: business solicitations; circumvention of export controls; and university research and product development; attendance at seminars and conventions; and acquisition of American companies.

Furthermore, in testimony before the House Judiciary Committee on September 18, 2007, Mike McConnell, the Director of National Intelligence, stated that "China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities and development projects, and their efforts are approaching Cold War levels."

The recent recalls and safety concerns with products imported from China, including pet food, toothpaste, and toys, should remind us that the United States is ultimately responsible for protecting its citizens from any and all threats. In light of China's expansive military modernization and its tremendous economic growth, we cannot afford to ignore the threat that espionage and cyber-attacks directed by China towards the United States poses to our national security.

I hope that you will consider this matter and act upon it as quickly as possible.

With kind personal regards, I am

Sincerely,

J. Randy Forbes
Member of Congress