Ranking Member Brian Higgins (D-NY) Opening Statement

"Iranian Cyberthreat to the U.S. Homeland"

Subcommittee on Counterterrorism and Intelligence &

Subcommittee on Cybersecurity, Infrastructure Protection, & Security Technologies

April 26, 2012

A cyberthreat is a threat that knows no limit and has no boundaries.

A cyber hacker does not have to fly a plane, get a visa, nor cross a border in order to create a devastating impact on our nation's economy and national security.

A cyber attack on the United States would transcend Congressional district lines and would not have any interest in partisanship.

According to the director of the Federal Bureau of investigation, Robert Mueller, threats from cyber espionage, computer crime, and critical infrastructure will surpass terrorism as the #1 threat to the United States.

The Director of National Intelligence, James Clapper, has stated that two of the greatest strategic challenges regarding cyber threats are: (1) definitive, real time attribution of cyber attacks—knowing who carried out the attack and where the perpetrators are located and (2) managing the vulnerabilities within the I.T. supply chain for U.S. networks.

In both cases, US Government engagement with private sector owners and operators of critical infrastructures is essential for mitigating these threats.

America's economic prosperity depends on cyber security, and that is why we need robust cyber legislation that includes strategic initiatives, including public-private partnerships that protect our nation's critical infrastructure from hackers, state actors, and foreign intelligence services from countries such as Iran.

According to the DNI, Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity. The DNI assesses that this will be one of the top threats to the United States in the coming years.

The former director of the National Counterterrorism Center, Michael Leiter has stated that a cyber attack from Iran is more likely than an attack on U.S. soil.

What makes a cyber attack on the United States so attractive to Iran, where the Internet is known to be heavily censored?

Despite Internet censorship in Iran, all major cities have full Internet service, and the depth and breadth of coverage is increasing rapidly.

Iranians have the desire to "plug in and play" to the world's marketplace of ideas. They are not immune to what is going on in other parts of the world, including the United States.

So what would motivate a cyber attack?

Would Iran's economic disconnect from the financial world be an attraction to gauge a cyber attack against financial institutions?

We know Iran's history of carrying out attacks via proxies. Does the ease of finding proxies to conduct cyber attacks make Iran more susceptible to carrying out a cyber attack than a kinetic one?

How can we know if the United States is prepared to handle a cyber threat from Iran?

Are our efforts strong enough? Do we need to require a government agency to give us updates on the technological advances that Iran is making with regard to cyber intrusions?

I, along with Congressman Duncan, who sits on this panel, have co sponsored a bipartisan bill that would require the State Department to provide updates on Iran's technological capabilities. Would that be helpful?

Although these are questions to which our witnesses can lend their thoughts, I would like to ask that the Subcommittee hold a classified Member Briefing to receive an update from the Intelligence Community on the Iranian cyberthreat so we can gain more understanding of what we face.

While the IC is not here to give us the specifics on the Iranian cyber threats, which would be inappropriate for this open setting. I would like to concentrate on what we know.

We know that Iran poses a threat to our cybersecurity. We also know that our information technologies have massive vulnerabilities. We know that our dependence on technology is growing exponentially by the day. We know that our moving forward as a nation depends on our having a robust, comprehensive cybersecurity policy in place.

Therefore, we must have legislation and policies that not only examine the threat, but also protect critical infrastructure and promote research and development that will ensure that we have the proper protocols in place to prevent a cyber attack.