

Eshoo Statement Urging Nomination of a Cyber Security Czar

September 13, 2006

Eshoo Statement Urging Nomination of a Cyber Security Czar

September 13, 2006

Washington, D.C. --Rep. Anna Eshoo, D-Palo Alto, delivered the following statement Wednesday at a hearing by the Energy and Commerce Subcommittee on Telecommunications and the Internet entitled "Cybersecurity: Protecting America's Critical Infrastructure, Economy, and Consumers."

"Thank you Mr. Chairman, and thanks to the witnesses for joining us today.

"As a member of the House Intelligence Committee, I take very seriously the range of threats to our country from terrorists and other enemies, including threats to the basic infrastructure of our telecommunications networks and the Internet.

"In the 21st Century, no part of our national infrastructure is more important than our technological infrastructure and communications networks.

"Former Cyber Security Czar Richard Clarke once described the potential for a telecom disaster as an 'electronic Pearl Harbor.' CRS has estimated a cyberattack could produce an economic blow exceeding \$200 billion.

"This is undoubtedly a shared responsibility of government, the telecommunications industry, business, and consumers, and critical gaps in security remain unaddressed at every level.

"I'm increasingly concerned that cybersecurity is not receiving the attention it requires from the federal government.

"In the wake of 9/11, the Administration has slowly diminished responsibility for and visibility of cybersecurity matters at the federal level. Instead, they have focused almost exclusively on threats to air safety and border security. These are critical threats to our national security but they are not the only ones. We must attend to all critical sectors, including cybersecurity.

"The position of Cyber Security Czar once resided at the White House and reported directly to the President, but after

Richard Clarke's resignation in 2003, the position was relegated to a mid-level position in the Department of Homeland Security.

"In July 2005, after significant pressure from Congress and the private sector, DHS Secretary Chertoff announced the creation of an Assistant Secretary for Cyber Security and Telecommunications. The Assistant Secretary would have the authority to set policy and develop public-private partnerships with industry to improve national cybersecurity.

"But in the year since the position was announced, the Administration has yet to even nominate someone to fill it.

"Clearly, we cannot expect national leadership in cybersecurity without an individual to lead the effort. I hope the President will act soon to appoint someone to assume this vital function.

"I also believe much of the responsibility for America's cybersecurity lies with the private sector and individual citizens.

"Many of the most potent viruses and worms that afflict our computer networks are able to do so only because the vast majority of personal computers are not secure, thus becoming the unwitting distribution network for destructive programs.

"Business and individuals must be vigilant in maintaining appropriate security on their networks and personal computers, and utilize sound security practices.

"The federal government should play a leadership role in promoting effective security standards and practices and assisting private and public institutions in reaching out to individual users to protect themselves from cyberattacks.

"Data security legislation unanimously endorsed by this Committee would provide significant government leadership in endorsing and promoting robust security systems and standards, and I hope the House will consider our bill before Congress adjourns.

"We have to do better than react to an 'electronic Pearl Harbor.' I look forward to working with my colleagues to make sure that we do everything we can to protect our nation's vital computer and communications networks."

##