Honorable Anna G. Eshoo

If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?

Answer: Comprehensive cybersecurity legislation that provides a legal framework for the nation to effectively address, across all departments of government and the private sector, the increasing cyber threats that are directed against the country and that probably will lead to a catastrophic event(s) for the nation.

Rationale: Today the nation suffers from increasing exploitation from criminal, hacktivist, nation-state, and terrorist groups directed against government and private sector critical infrastructures and business interests. In addition, nation-states are conducting cyber economic espionage against the U.S. to obtain business plans, source code, innovation, research and development and other valuable intellectual property for competitive advantage over the country. In time, some nation state or terrorist group will use the 1000's of malware attack tools generated annually by nation states in preparation for potential cyber-war for a destructive attack against the U.S. Examples include attacks to degrade or destroy liquidity and confidence in the global banking system, electric power distribution or mass transportation. We have the capabilities to slow down or halt such exploitation or direct attacks, however, we do have the legal framework in place that allows and, in fact, requires the needed collaboration and sharing of sensitive information from government to the private sector, between private sector entities and from the private sector to government. There were many bills and amendments proposed in the Congress last year. None of them were successful in passing both Houses of the Congress for signature by the President. This failure leaves the U.S. vulnerable as we become increasing digitally dependent.

Mike McConnell