Affidavit In Support of Search Warrant Application

I, Eric Sims, Agent of Homeland Security (DHS), being duly sworn, depose and say:

1. I am currently assigned to the Ruston Division of the DHS where my duties include investigating acts of terrorism and cybercrimes.

2. This affidavit is in support of an application for a warrant authorizing the National Security Agency to provide DHS with all communications and data pertaining to the attack on Washington D. C.'s transportation systems and individual vehicles. We specifically would like the NSA to obtain the day passing through the tor exit node cluelessclue - 173.132.211.248 which is located in the District of Columbia.

3. The items requested to be discovered are as follows:

1. All communication data including ip addresses, port numbers, times, and obtainable content destined for General Motors OnStar in car information system as well as DC Metro's network.
2. Identity of the registrant associated with the originating IP addresses that are discovered by analyzing the tor exit node 173.132.211.248.

Factual Background

1. This case involves hacking of GM vehicles manufactured after 2010 as well as the network that supports the DC Metro system. A hacker has managed to cause the halt of the Metro system as well as cause several GM vehicles to malfunction. This malfunction causes the cars to turn off causing drivers to loose all power. The result is many accidents causing gridlock on the streets of DC. We must obtain the data outlined above to locate the person that attacked our nation's capitol.

2. We are asking for authorization for the NSA to analyze the traffic exiting the tor node cluelessclue because the tor network is intentionally designed to obfuscate a users identity and location. The tor network works by randomizing the path of data through a set of nodes and striping the original data of the IP address from which it originated. The NSA has developed methods by which they are able to obtain the information from a particular exit node if the node is known.

3. We are specifically asking for the exit node 173.132.211.248 in the District of Columbia for several reasons. The first factor in our decision is the node's geographical proximity to the location in which the attacks occurred. The second factor in our decision is we believe the perpetrator of this act to also be in DC. As the Metro was currently being upgraded we expect that it must be someone familiar with the ATO system that is being implemented this summer. The attacker would also have to have sufficient technical ability to compromise the GM OnStar system. We expect that the IP address will be linked to Chrissy Paxton due to her expertise in both areas.

4. We believe the result of the execution of this warrant will be the discovery of the IP address from which the attacks where launched as well as the location and owner of the IP address. This evidence will be used in the capture of the hacker that perpetrated these acts on Washington DC.