UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

(Name, address or brief description of person or property to be searched)

“Cluelessclue”

IP Address: 173.132.211.248, located in Washington D.C.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

We, Team 6 NOMMA, Agents of the Department of Home Security (DHS), being duly sworn, depose and say:

1. We are currently assigned to the Louisiana Tech University Division of the DHS where our duties include investigating threats to national security.
2. This affidavit is in support of an application for a warrant authorizing IP Address: 173.132.211.248 to provide law enforcement with any and all means of gaining access, including the origins of the exit node, emails, email contacts, and/or messaging contacts, in order to obtain the complete contents of the suspected perpetrator

4. The Items Requested to be seized are as follows:

a. We expect to find the originating location of the TOR encryption as well as the device who sent the attack.

b. We expect to find the web browser history as well as trace evidence which we can piece together in order to construct the origin computer's e-mail and messaging history, including but not limited to; Tinder, E-Harmony, Discord, and other private messaging apps.

FACTUAL EVIDENCE

DHS analysis of network traffic from the DC Metro and OnStar attack today concluded that both attacks were directed through the TOR network to obfuscate the originating location. Given the nature of the TOR network, no exacting location can be determined. However, DHS agents were able to limit the scope for the exit node used by the attackers to three possible locations.

To understand why we are requesting information from this particular IP address, a brief explanation of the TOR network must be given. TOR is a network of encrypted nodes used to bounce and encrypt information around the world in order to anonymously send and receive information. The user sends

information through TOR via an entry node. The information is then given to another node, which then bounces to numerous other nodes in succession, encrypting the file and its origin location. The information is finally sent to an exit node, which decrypts the node back into clear text. It then proceeds along the unencrypted internet to its final destination.

We chose the IP address based in Washington DC because this is where the Metro and OnStar attacks occurred. The other two suspect IP addresses have exit nodes in Detroit and Boston, which are far removed from the location of the address.

DHS needs the information from this IP address in order to run a traffic pattern analysis in order to determine the origin of this threat.