AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

We, as members of the DHS, being duly sworn, depose and say:

1. We are currently assigned to the DHS where our duties include investigating threats to national security.

The items requested to be seized are as follows:

a. KRISTOF REIMERINK'S computer and the ability to copy any files on the computer off site.
b. All network logs on KRISTOF REIMERINK'S computer from the date of February 14, 2016, to June 24, 2016, account login and password information and other identifying information.
c. All emails sent and received between February 14, 2016, to June 24, 2016, and personal contact list information stored on the computer.
d. Provide times and duration of the user's access on the internet and, if applicable, any web pages visited as well as any Internet Protocol (IP) addresses accessed between February 14, 2016 to June 24, 2016.

FACTUAL BACKGROUND

1. This case involves KRISTOF REIMERINK as a primary suspect of the transportation hijack in the District of Columbia. REIMERINK has a profound interest in computer technology; he currently attends MIT, where he studies Computer Science.
2. REIMERINK has a history of computer hacking. His work to remotely hack into automobile systems in 2014 demonstrates his skill.
3. In the past, REIMERINK has been known to work with cartel groups, such as Sinaloa and Lobos Juarez. The suspect commonly involves himself in illegal behaviors.
4. He operates online with the handle Rhyme or Reason. This same user name is listed as a suspected member of the Sleeperz hacking group.
5. The Sleeperz is a mercenary hacker group typically hired by foreign nationals like Iran. This group has "hacked and defaced 256 government websites." Sleeperz is also suspected of hacking into and modifying the public transportation system in Boston, MA.
6. In recent months, REIMERINK has been exchanging emails with a member of the Iranian embassy, via the email address alirezasolsimani@ir.gov. The emails imply that REIMERINK and the Iranians have exchanged packages. In addition to this, he claims to have recently received a large sum of money from an unknown source.
7. In February 2016, REIMERINK sent an email to jacobhacks@bigbobsbeautifulbentleys.com on the topic of purchasing an older model car that did not possess the technology used to disable the automobiles in the DC attack.
8. The NSA has determined that a TOR exit node located in Boston, MA, was likely involved in the attack on Washington's transportation.

9. REIMERINK is familiar with the hacking and use of TOR networks. He references this in an email to Di Ni with the hashtag “torhack.”

ATTACHMENT A

The laptop/personal computer of Kristof Reinerink should be taken from his apartment at 18 Laurel Street, #A, Boston, MA 02119.

ATTACHMENT B

Through this warrant, we are expecting to discover Kristof’s connection to the attack on the DC transportation system that occurred the morning of June 24, 2016. Kristof’s emails between February 14, 2016, and June 24, 2016, should indicate that he received payment to create a TOR node as well as providing information about how vulnerabilities in automobiles can be exploited. Reviewing the network logs will provide the IP addresses which will then lead us to the person(s) who executed the attack and in addition prove that his computer and its TOR exit node was used in the DC transportation incident.