AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

We, Special Agents (SA) of the Department of Homeland Security (DOH), being duly sworn, depose and say:

1. We are currently assigned to the Computer Crime and Intellectual Property Office at DHS where our duties include investigating cyber crimes and cyber terrorism.
2. This affidavit is in support of an application for a warrant authorizing PETER BISHOP, as described in Attachment A, to provide law enforcement with any and all means of gaining access, including login and password information, password reset, email contact list, email contact information, and the contents of an and all email accounts, both personal and professional, belonging to Mr. Peter Bishop.

3. The items to be seized are as follows:
    a. Provide any additional email addresses and IP addresses associated with Mr. Peter Bishop including but not limited to pbishop@emory.edu.
    b. Provide email contact list and contact information associated with all email addresses on file for Mr. Peter Bishop including but not limited to pbishop@emory.edu.
    c. Provide the contents of all email accounts associated with Mr. Peter Bishop including but not limited to email logs with documented dates, times, and IP addresses, recipients of the emails with documented dates, times, and IP addresses, calendar obligations, and notes beginning July 13th, 2015 and ending July 25th, 2015.
    d. The location, property, and records to be searched are located at and described as: Peter Bishop at Emory University of Medicine at 1617 Clairmont Road NE, Decatur, GA 30033.

Using the Cyber Discovery Toolkit and the program Wireshark, members of the team were able to analyze the communication log files from the Astrapi system on July 24th, 2015, the day that three cars were lost from the Crimson Bullet.

In the communication logs, several attempts were made from the IP address of Dr. VirDau (130.207.188.52) to acquire secure authentication in the Astrapi system. At 12:38 am PDT and 1:10 am PDT, secure access was granted and sensor data about cargo going from Infinity BioGen to REM was retrieved. Upon further investigation, a third attempt was made at 4:00 am PDT to connect from the same IP address. This request for access was also granted; however, before sensor data could be obtained, the connection was severed by request of the user. Immediately after logging out, between 4:02am and 4:11am, 100 attempts to secure authentication were made from the same

IP address and failed. On the 100th try, access was granted and a command to disable SELinux, the Astrapi system security program, was sent. One executable file was sent in the seconds following from the same 130.207.188.52 IP address.

Also at 4:11 am PDT, but following the aforementioned actions, a second executable file was sent from the IP address of Mani Ramachandran Subra from NIC, A-Block CGO Complex, New Delhi, India (164.100.56.202). An execute command was sent 33 times between 4:11am PDT and 9:05 am PDT from this IP address. Members of the DHS Cyber-Crime Joint Task Force analyzed the executable code and determined that Subra's IP address was used to directly communicate with the Astrapi system via system port 1 and the execute code caused the Astrapi system to report incorrect GPS data to the DOT. This inaccurate data made the train appear to seem as if it was moving along the prearranged path while it was in actuality moved to another location.

At 9:05 am PDT, the Astrapi system initiated a reboot because it detected an instability in the system, but until the reboot all communication to and from the train was blocked except faked system reports sent to the DOT. Using information gathered by the FBI Cyber-Crimes Division and the Organized Crime Division, Mr. Subra's IP address is also connected to the hacking group "IndieShell" and to the cartel "Sunset Boyz".

We have reasonable cause to believe Peter Bishop, a student worker for Emory's campus IT, is connected to the hacking event at REM that took place on July 24th, 2015. Peter Bishop is an active member of PETA, along with his colleagues Sandra Bullock, Donald Webre, and Raphael Sabmud. Peter is also an active member of the group "Better Living without Chemicals," which is a group that strives to "resist the encroachment of science and manufacturing in our lives today." Better Living without Chemicals ideals is at odds with the REM's endeavors to "transform the treatment of new technologies" ("Mission").

On July 24th, 2015, we discovered an email chain between Bishop and his colleagues that we feel connect him to "IndieShell" case. In the emails, Peter urges his friends to meet and join "PETA against the proposed camel research" because "the terror won't stop until they [we] speak up."

In an email dated July 3rd, 2015, one of Peter's colleagues, Sandra Bullock referred to their targets as, "capitalist pigs. Let's hope they get some pig virus." While never directly stating their intentions, this references their desire to spread the deadly super virus that they secured on the Crimson Bullet eleven days later. Raphael responds to this email praising Sandra and uses the hashtag "timeforatrainwreck" indicating the connection to the crimson bullet.

We believe that the group’s disillusionment with the unethical treatment of animals in an attempt to reap more profit led them to take action and make a statement by securing the virus on the train and infecting the majority (50-100%) of the population in only 3-4 days (“Pathogen Safety Data Sheet”). This relentless pursuit of justice is consistent with IndieShell’s motto, “We never forgive. We never forget.”