From our team’s research on the drone attack in Turkey, we have found that the Kentucky Institute of Technology (KIT) is in violation of 18 U.S.C. SECTION 1030 (accessing a computer and obtaining national security information). We have established probable cause by way of verifiable information received by our group of agents. We feel as if receiving electronic information from KIT would further our knowledge about the connection between Khalid Mehmet and Turkish General Necdet Ozel. Khalid is a director in the Advanced Systems Center at the Kadir Has University. General Necdet Ozel is his nation’s highest ranking military commander, who we feel is behind the recent drone attacks in Turkey. As a result of receiving this information we feel as if we can establish probable cause for a warrant application from two sources: the memos identifying faulty equipment and the contract which had the goal to reprogram the faulty equipment. As a result of the contract not reaching its’ goal of correcting the flaw in the software, we believe Khalid Mehmet turned the contracted access of the drone information into illegally obtained intelligence, because of access to the drone’s original specifications and software files.

Back in March of 2012, Drone Inc. released an email regarding the STM- 7007 chipset. The email was sent to KIT and other companies regarding the fact that STM chipsets had design flaws. According to Drone Inc., “The chip-STM-7007 cannot effectively make use of AES encryption.” The problem appeared when used for certain missions. Drone Inc. warned users to quickly evaluate and resolve the problem with the chip. Military chip users were told to contact the Drone Inc. Vice-President for help. Ignoring the problem would prove catastrophic: a problem that Turkey and the U.S. would learn the hard way.

In 2013, the Kentucky Institute of Technology offered a new contract to a variety of employees. These employees included Khalid Mehmet, Frank Furter, Jean Gourd, Earnest Borgine, Tim Cury, and Isaac Hayes. The contract was created to fix the bad chip by fully reprograming the chip to ensure a fully operational device. The workers’ exact job composed of “completing all coding necessary to implement a fully functional AI control system”. Weekly updates were to be submitted to Jean Gourd, who verified that all of the coding was functional and error free and all coding was to be completed by August 18th, 2013.

The chip company, STM, composed a document in 2014 identifying trouble codes that the STM-7007 was still experiencing. In the document dated 4/1/14 STM finds the failure of the chip to be “During handshaking for TLS communication, AES is sent as a supported algorithm. TLS connection procedures are able to finalize successfully but the data streams falls back to using DES on transmission. The algorithm switch is processed properly with the TLS protocol so communication is never interrupted” (“AAT-13.” Errata sheet. STMicroelectronics, 4/1/2014). As a result, our agents concluded the five employees in the 2013 contract did not fix the encryption issue on the chip. The chip still could not make use of the AES encryptions. Afterwards, STM requested to replace the bad chip with a revised STM-7007b model device.

As DHS agents, we strongly believe the information in this document strongly supports our case to obtain a warrant. This warrant would be used to search the Advanced Prototyping Lab in KIT. The warrant would allow DHS to immediately gain electronic information and evidence of the programming code on the 2013 chip and emails from the 2013 team.