Contact:
Brian Hart, President
Black-I Robotics, Inc.
brian@blackirobotics.com
www.blackirobotics.com
141 Middlesex Rd. Suite 4
Tyngsboro, MA 01879
O: 978-703-1236

FOR IMMEDIATE RELEASE

Black-I Robotics Wins Air Force Contract to Help Secure Robots from Hackers

Tyngsboro, Mass. July 25, 2012 – Black-I Robotics, Inc. has won a contract from the Air Force Research Laboratory in Rome, NY to supply unmanned ground vehicles and related consulting services. The program will make unmanned vehicles and automobiles more secure and safe from cyber hackers and thus safer.

ABOUT THE AIR FORCE CONTRACT. Black-I Robotics will provide unmanned ground vehicles and consulting services to the Air Force in support of a Defense Advanced Research Projects Agency (DARPA) program. Black-I's contract amount is $528,000 for the initial delivery to be completed in October 2012. The contract was officially posted 10 July. Black-I Robotics will locally build three LandShark Series H unmanned ground vehicles (UGVs). These vehicles will consist of an advanced and proven LandShark mid-sized unmanned ground vehicle (UGV), an operator control unit, a military radio system and several special payloads for the DARPA project. Initial payloads will be a mobile turret, anti-collision radar system and an advanced sensing platform with high-end optical and thermal imaging cameras.

ABOUT THE DARPA HACMS PROGRAM. The DARPA program, sponsored by the Air Force, is called High-Assurance Cyber Military Systems or more commonly "HACMS".

Iran Caught a Drone. It was funded by the Air Force shortly after Iran caught a US unmanned spy drone in late 2011 – the RQ-170 Sentinel –purportedly by hacking and spoofing its GPS and computer systems causing it to land in Iran. Air, ground, water surface, and underwater unmanned systems; commonly called drones, unmanned systems or robots; are likewise vulnerable to cyber attack of various kinds. "Using robotic vehicles against uneducated combatants is one thing, using them against nation-states is quite another" said Brian Hart, President of Black-I Robotics.

Automobile Hacking. Automotive safety and privacy vulnerabilities emerged last year, as reported in the New York Times. Automobile electronics, communications and navigation systems where hacked to gain control of vehicle engines, brakes and other controls. Car and Driver reported in August 2011, "Currently, there's nothing to stop anyone with malicious intent and some computer-programming skills from taking command of your vehicle. After gaining access, a hacker could control everything from which song plays on the radio to whether the brakes work." Hart said, "It is only a matter of time before malicious individuals exploit these automotive vulnerabilities."

Simulated Attacks. DARPA will be announcing late this month, red and blue team winners that will use Black-I's robots for a three phase 4 ½ year program. Red teams will attack the LandShark UGV simulating an enemy such as an advanced nation-state or malicious hacker. Blue teams will defend, working to upgrade hardware and software, to prevent the Red teams from gaining control or disrupting the robot's operation. Research participants that will use these robots are expected to include major US research universities, government labs and automotive companies. Those selected should be announced later this month by DARPA.

WHY BLACK-I AND THE LANDSHARK UGV. "Black-I Robotics was selected by DARPA and the Air Force because it uses an open-architecture configuration specified for military systems on a user friendly and modifiable mid-sized robot. "Many unmanned ground vehicles are simply too small for research purposes or lack adequate computer intelligence. Larger ATV or Humvee sized robots are too dangerous. Likewise, unmanned aerial systems make poor choices for hacking research because loss of control causes catastrophic crashes. The LandShark UGV weighs between 500-800 lbs and while very powerful for outdoor field reconnaissance, is still small enough to go indoors through a door frame," said Hart.

Advances derived from this program will likely be integrated by Black-I into future robot designs as the program evolves which should put Black-I Robotics front and center in the emerging cyber-secure robot environment. "It is evident that older robotic systems are vulnerable to electronic or cyber attack," said Hart.

TURRET WITH SIMULATED WEAPONS. For this project Black-I is developing a robust firing turret that can be activated remotely by an operator. "Any future weaponized robots will have to be secure from outside meddling to prevent them from being turned on their masters. For safety purposes we are mounting on the turret a remotely fired paint-ball gun to simulate a weapons system," said Hart. These initial units are likely to go to major research universities.

AUTOMOTIVE ANTI-COLLISION RADAR. The radar systems which will be mounted on the robots are used in automobiles as anti-collision systems which may one day be the basis of autonomous automobiles. "Keeping automotive anti-collision systems and other components secure from outside hacking is part of this project with obvious relevance to automobile safety," said Hart.

HIGH-END CAMERA AND THERMAL IMAGING ARRAY. The high-end camera and thermal imaging array is used regularly on military vehicles and border security structures. "Robots have emerging applications as border patrol scouts or base perimeter guards, but losing control of the camera array to an enemy would be catastrophic," said Hart. This program will help secure those systems.

ABOUT BLACK-I ROBOTICS. Black-I Robotics was founded in 2005 by brothers Brian and Richard Hart to make affordable robust mid-sized unmanned ground vehicles. Black-I is located in Tyngsboro, Massachusetts, and is a small privately owned business. Black-I has worked with all branches of the military and most particularly with the counter-terrorism elements of the Department of Defense that focuses on dual-use technologies for military, law enforcement and public safety applications. "If it weren't for the Counter Terrorism Technology Support Organization's Technology Support Working

Group (TSWG), our LandShark UGV program would never have unfolded," said Hart. "TSWG is a small and nimble agency whose critical counter-improvised explosive defeat capabilities are slated to be defunded by the Senate for FY2013 which will quickly erode our nation's law enforcement counter IED capabilities to pre-911 levels with grave consequence," said Hart.

XXX