Press Advisory

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

410-981-6610 ● challenge@dc3.mil

FOR IMMEDIATE RELEASE May 27th, 2010

2010 DC3 Digital Forensics Challenge Partners with John Hopkins Carey Business School and CyberWatch

LINTHICUM, Md. — The Department of Defense Cyber Crime Center's (DC3) Digital Forensics Challenge has partnered with John Hopkins Carey Business School and CyberWatch for the 2010 Digital Forensics Challenge. As part of one of three original U.S. Cyber Challenges, the DC3 Digital Forensics Challenge is an annual call to the digital forensics community to pioneer new investigative tools, techniques, and methodologies.

The 2010 DC3 Challenge encourages innovation from a broad range of individuals, teams, and institutions to provide technical solutions for computer forensic examiners in the lab as well as in the field. Approximately 20 different challenges ranging from basic forensics to advanced tool development are being provided to all participants for the challenge. The challenges for 2010 are single based challenges and are designed to be unique and separate from one another. This format is different than the whole forensic process scenario, with incorporated challenges, provided for the 2009 DC3 Challenge.

In sponsorship with DC3, the Johns Hopkins Carey Business School and CyberWatch (JHU/CW) will be offering an additional prize in 2010 DC3 Digital Forensics Challenge. This competition prize will be open to all students attending U.S. community colleges in the United States as a participant of the DC3 Challenge.

To qualify for this prize within the 2010 DC3 Challenge, teams must list their community colleges per team member as their school. The winning team will be recognized as the academic leader at the community college level. The winners will also be presented with an award to mark their outstanding achievement.

The 2010 DC3 Digital Forensics Challenge now has near 600 teams comprised of both domestic and international team members. The

participating teams include 400+ domestic teams, 180+ international players and 30+ teams with mixed U.S. and non-U.S. citizenships. A total of 43 non-U.S. countries have representation as well as 47 U.S. states.

“I’m excited that Johns Hopkins Carey Business School and CyberWatch have partnered with DC3 to encourage the 2-year institutions to develop digital forensics curriculum and to mentor the students interested in this critically important field”, said Special Agent (Retired) Jim Christy, Director of Futures Exploration at DC3.

About Johns Hopkins Carey Business School (http://carey.jhu.edu/):

With a history of educating business leaders since 1916, the Johns Hopkins Carey Business School (JHU) specializes in creating innovative programs that anticipate and reflect global business trends. The School also draws upon the strengths of other Johns Hopkins schools, including the Johns Hopkins Bloomberg School of Public Health, the School of Medicine, School of Nursing, the Whiting School of Engineering, and the Zanvyl Krieger School of Arts and Sciences.

About CyberWatch (http://www.cyberwatchcenter.org/):

CyberWatch (CW) is a consortium of higher education institutions, businesses, and government agencies focused on building and maintaining a stronger information assurance workforce. Consortium participants collaborate to share best practices, methodologies, curricula, and course modules and materials. It is an Advanced Technological Education (ATE) Center, headquartered at Prince George’s Community College, and funded by a grant from the National Science Foundation (NSF). The CyberWatch goals are focused on information assurance (IA) education at all levels, from elementary through graduate school, but especially the community college level, and include curriculum development, faculty professional development, student development, career pathways, and public awareness.

About DC3 Digital Forensics Challenge (http://www.dc3.mil/challenge):

The DC3 Digital Forensics Challenge’s purpose is to promote and generate interest in digital forensics; establish relationships within the digital forensics community; address the major obstacles and dilemmas confronting digital forensics investigators and examiners; and develop new tools, techniques, and methodologies. It is hosted by the Department of Defense Cyber Crime Center with sponsorships and partnerships from the Digital Forensics community.

###