DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL
1600 DEFENSE PENTAGON
WASHINGTON, DC 20301-1600

MAY 15 2009

The Honorable Nancy Pelosi
Speaker of the House of Representatives
Washington, DC 20515

Dear Madam Speaker:

The Department of Defense requests that the Congress enact the enclosed legislative proposal as part of the National Defense Authorization Bill for Fiscal Year 2010.

The purpose of the proposal is stated in the accompanying section-by-section analysis.

The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presenting of this legislative proposal for your consideration and the consideration of the Congress.

Sincerely,

Jeh Charles Johnson

Enclosure:
As stated

DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL
1600 DEFENSE PENTAGON
WASHINGTON, DC 20301-1600

MAY 15 2009

The Honorable Joseph Biden
President of the Senate
Washington, DC 20510

Dear Mr. President:

The Department of Defense requests that the Congress enact the enclosed legislative proposal as part of the National Defense Authorization Bill for Fiscal Year 2010.

The purpose of the proposal is stated in the accompanying section-by-section analysis.

The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presenting of this legislative proposal for your consideration and the consideration of the Congress.

Sincerely,

Jeh Charles Johnson

Enclosure:
As stated

**SEC. ___. DEFENSE CYBER CRIME CENTER: AUTHORITY TO ADMIT PRIVATE SECTOR CIVILIANS TO CYBER SECURITY COURSES.**

(a) AUTHORITY FOR ADMISSION.—The Secretary of Defense may permit eligible private sector employees to receive instruction at the Defense Cyber Investigations Training Academy operating under the direction of the Defense Cyber Crime Center. No more than the equivalent of 200 full-time student positions may be filled at any one time by private sector employees enrolled under this section, on a yearly basis. Upon successful completion of the course of instruction in which enrolled, any such private sector employee may be awarded an appropriate certification or diploma.

(b) ELIGIBLE PRIVATE SECTOR EMPLOYEES.—For purposes of this section, an eligible private sector employee is an individual employed by a private firm that is engaged in providing to the Department of Defense or other Government departments or agencies significant and substantial defense-related systems, products, or services, or whose work product is relevant to national security policy or strategy. A private sector employee remains eligible for such instruction only so long as that person remains employed by an eligible private sector firm.

(c) PROGRAM REQUIREMENTS.—The Secretary of Defense shall ensure that—

(1) the curriculum in which private sector employees may be enrolled under this section is not readily available through other schools; and

(2) the course offerings at the Defense Cyber Investigations Training Academy continue to be determined solely by the needs of the Department of Defense.

(d) TUITION.—The Defense Cyber Investigations Training Academy shall charge students enrolled under this section a rate that is at least the rate charged for employees of the United States, including overhead.

(e) STANDARDS OF CONDUCT.—While receiving instruction at the Defense Cyber Investigations Training Academy, students enrolled under this section, to the extent practicable, are subject to the same regulations governing academic performance, attendance, norms of behavior, and enrollment as apply to Government civilian employees receiving instruction at the academy.

(f) USE OF FUNDS.—Notwithstanding section 3302 of title 31, United States Code, or any other provision of law, amounts received by the Defense Cyber Investigations Training Academy for instruction of students enrolled under this section shall be retained by the academy to defray the costs of such instruction. The source, and the disposition, of such funds shall be specifically identified in records of the academy.

**Section-by-Section Analysis**

This section would authorize the Secretary of Defense to permit eligible private sector employees to receive instruction at the Defense Cyber Investigations Training Academy operating under the direction of the Defense Cyber Crime Center. The Defense Cyber Crime Center (DC3) was established on October 1, 2001, incorporating the newly-created Defense Cyber Crime Institute with the existing Defense Computer Investigations Training Program and the Defense Computer Forensics Lab.

DC3 is the Department of Defense (DoD) center of excellence to efficiently organize, equip, train, and employ scarce resources to more effectively address the proliferation of computer crimes affecting the DoD. DC3 is responsible for providing digital evidence processing, analysis, and diagnostics for any DoD investigation that requires computer forensic support to detect, enhance, or recover digital media (including audio and video). Such investigations include criminal, counterintelligence, counterterrorism, and fraud investigations of Defense criminal investigative organizations and DoD counterintelligence activities.

Through the Defense Cyber Investigations Training Academy, DC3 provides computer investigation training to forensic examiners, investigators, system administrators, or any other DoD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation.

The Department maintains strong government-to-industry relations through collaboration on cyber/network security through bilateral agreements in the DoD-Defense Industrial Base Cyber Security/Information Assurance Program. This program works with Defense Industrial

Base partners to improve cyber security and to secure information systems from unauthorized use, counterintelligence and criminal and fraudulent activities, on unclassified systems owned or operated by these partners, and on which defense-related unclassified information resides. Defense Industrial Base partners provide products, services and capabilities of significant and substantial importance to the Department of Defense and other Government departments and agencies (*e.g.*, aeronautics, armaments, biological and chemical technologies, electronics, information technology systems and services, telecom systems and services, nuclear components and capabilities, space systems, energy systems, strategic analysis capabilities, weapons, etc.). In order for this cyber security/information assurance effort to be truly effective, the Department should make available training to industry partners in the areas of computer investigation techniques and procedures

This legislative language is modeled after 10 U.S.C. 2167, which authorizes private sector civilians who work in organizations relevant to national security to receive instruction at the National Defense University on a reimbursable basis.

**Changes to Existing Law:** This proposal would not make any changes to existing law.