U.S. DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY ADVISORY COUNCIL

November 14, 2012

Chair:
Judge William Webster

Vice Chair:
Chief William Bratton

Members:
Norman Augustine
Leroy Baca
Chuck Canterbury
James Carafano
Lawrence Cockell
Jared Cohon
Ruth David
Mohamed Elibiary
Ellen Gordon
Lee Hamilton
Jim Jones
Raymond Kelly
Carie Lemack
Wilson "Bill" Livingood
John Magaw
Walter McNeil
Matt Mead
Bonnie Michelman
Jeff Moss
Martin O'Malley
Annise Parker
Harold Schaitberger
Ben Shelly
Ali Soufan
Lydia Thomas
Frances Fragos Townsend
Chuck Wexler
John "Skip" Williams

Secretary Janet Napolitano
U.S. Department of Homeland Security
Washington, DC 20528

Dear Madame Secretary:

The Task Force on CyberSkills was created in response to your tasking on July 2, 2012, to the Homeland Security Advisory Council (HSAC). Over three months, the Task Force conducted extensive interviews with experts from government, the private sector, and academia to answer its two-part tasking: first, identifying the best ways that DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges, and second, outlining how DHS can improve its ability to recruit and retain that sophisticated cybersecurity talent.

The Task Force developed eleven recommendations grouped under five objectives (see pages 3 and 4 of the recommendations). I would like to highlight a few key pieces from these recommendations:

- **Mission-critical skills:** Recommendation 1 establishes a list of 10 mission-critical cybersecurity skills that are specific to the DHS mission. This will allow DHS to quickly define and prioritize the hands-on skills its workforce needs.

- **Proficiency testing:** Recommendations 2 and 3 establish a process by which to ensure the proficiency of DHS cybersecurity personnel. All personnel who are performing mission-critical tasks would be subject to recurring, scenario-based proficiency testing.

- **"Talent judging talent" model:** Recommendation 4 establishes several mechanisms to ensure that DHS' best cyber professionals are at the forefront of improving and developing the cyber workforce. This recommendation creates a Department-level infrastructure to develop and oversee the cybersecurity workforce and further specifies that the most talented professionals should define needed skills, train and mentor, and recommend new opportunities for cybersecurity professionals.

- **"Branding" Campaign:** Recommendation 5 focuses on the need for DHS to engage in a holistic "branding" campaign. Branding can establish public

recognition, build pride and ownership in the current workforce, and turn every "touch" into a recruiting and public relations opportunity. This recommendation can build upon the work of the Office of Academic Engagement to develop an Academic Speakers' Bureau that allows DHS officials to introduce students to the mission of and work at DHS.

- **Community Colleges:** Recommendation 6 and 8 propose a robust community college program in partnership with the Departments of Labor and Veterans Affairs. Community colleges have the ability to adopt new curriculum quickly, and DHS has the opportunity to work with these schools to ensure that they are producing enough people with the necessary hands-on cybersecurity skills.

- **Veterans:** In addition to the community college program open to all, the Task Force recommends particular focus on training and recruiting veterans (Recommendation 8). Veterans' operational experience makes them well-suited to cybersecurity work, and DHS can work with Veterans Affairs to assist this population in attending community colleges and subsequently finding employment at DHS.

- **Competitions:** The Task Force recommends that DHS sponsor a national competition that would serve as part of entrance requirements to the community college program (Recommendation 8).

- **CyberReserve:** The Task Force recommends that DHS start a pilot CyberReserve program to ensure that a cadre of DHS alumni and other cybersecurity experts will be known to DHS and able to be called upon if the nation faces a major cyber crisis. Much technical talent resides in the private sector, and the nation will be able to respond more effectively to a crisis if all available talent is utilized.

Sincerely,
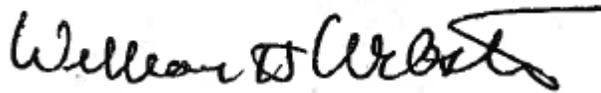
William Webster
Chair, Homeland Security Advisory Council