FACT SHEET
DHS Cybersecurity Mission – Veterans Outreach

Current Threat Landscape

America's daily life, economic vitality, and national security depend on a secure cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering homes, running the economy, and obtaining government services. No country, industry, or individual is immune to cyber risks. Malicious cyber activity has increased dramatically over the last decade to include attacks on financial and other data management systems, corporate strategy and trade secrets, and government networks that control our critical infrastructure.

DHS Cybersecurity Mission

DHS has the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems. DHS advances this mission through several of its Components such as the National Protection and Programs Directorate, the Science and Technology Directorate, U.S. Coast Guard, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the U.S. Secret Service. DHS is responsible for strengthening the nation's cyber infrastructure by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats. DHS leads efforts to protect the federal ".gov" domain, the private sector ".com" domain and conducts 24/7 cyber monitoring through the National Cybersecurity and Communications Integration Center.

DHS Cybersecurity Initiative

DHS recognizes the nation's growing cyber threat and has launched an initiative to further our cybersecurity mission and to ensure America has the world-class cybersecurity workforce needed to protect the information, systems, and networks that enable effective and secure operation of government and commercial elements of critical infrastructure. To achieve this mission, DHS efforts include:

1. ***Creating and implementing standards of performance*** – DHS is establishing a baseline of existing cybersecurity skills, assessing and defining workforce requirements, and developing a framework to ensure personnel are trained, hired, and tested for the appropriate cybersecurity mission-critical skill level.

2. ***Expanding and leveraging a national pipeline of highly qualified candidates for mission critical cybersecurity jobs*** – DHS is growing the pipeline by conducting sustained outreach with veterans, re-profiling standards for National Centers of Academic Excellence (CAEs), and implementing cyber intern opportunities which provide hands-on experience to students.

3. ***Institutionalizing strategic management of DHS' cybersecurity workforce*** – DHS is establishing strategic management of the cyber workforce across the Department as well as a Department-wide oversight body called "The Cyber Workforce Coordinating Council" to better coordinate workforce planning, recruitment, staffing, evaluations, training, and Cyber Reserve.

Commitment to Veterans

DHS has a strong commitment to hiring veterans and has exceeded the Fiscal Year 2012 (FY12) goals set forth by the President's Council on Veterans Employment. The final FY12 results for DHS reflected 24.9% veterans and 8.2% disabled veterans among all new hires, compared to the Council's goals of 21.8% and 8.2% respectively for DHS. DHS has also exceeded an internal goal of employing fifty thousand veterans across the Department. As of FY12, DHS employed nearly fifty five thousand veterans, just over 27% of the civilian workforce. The DHS Veterans Employment Program Office actively coordinates throughout the Department and with strategic partners to promote employment of veterans at DHS.

How Veterans Can Help Protect the Nation's Cyber Space

America owes a debt to veterans and recognizes they represent a unique pool of candidates due to their proven talent and commitment to public service. DHS can assist in building the nation's cyber workforce pipeline, and support our veterans at the same time, by enhancing opportunities for veterans to be educated and hired in mission-critical cybersecurity jobs.

Cybersecurity Careers
For veterans who have experience in cybersecurity, DHS offers exciting and dynamic careers in cybersecurity and the opportunity to be part of a world class cyber workforce. Information on cybersecurity careers at DHS can be found at http://www.dhs.gov/join-dhs-cybersecurity or at www.usajobs.gov (keyword: cyber).

Cybersecurity Education
For veterans who are looking to gain knowledge and education in cybersecurity, there are cybersecurity programs across the country that have been approved by the Department of Veterans Affairs (VA) for use of various veteran educational benefits. For more information on cybersecurity education, visit The National Initiative for Cybersecurity Careers and Studies at http://niccs.us-cert.gov/home/veterans.

VA offers various educational benefits that veterans may use to obtain a Cyber Security degree or certificate. Visit www.gibill.va.gov to learn more about available educational benefits provided through the VA.

Points of Contact and Additional Resources:
DHS – Monica Flint, Veterans Employment Program Specialist Monica.Flint@hq.dhs.gov
VA – www.va.gov and www.vaforvets.va.gov

Homeland Security