Thursday, November 19, 2009

MEMORANDUM FOR: Chief Human Capital Officers

FROM: John Berry, Director

Subject: Information Request for Cybersecurity Competency Models

The U. S. Office of Personnel Management (OPM), the Chief Information Officers (CIO) Council and the Chief Human Capital Officers Council of Workforce Development Subcommittee recently identified cybersecurity related occupations as high priorities for Governmentwide competency models. OPM is pleased to kick-off the development of these models. This initiative will identify the critical elements of success for the covered workforce, ensuring classification, selection, development, and performance management programs are based on a valid framework.

We are collaborating with the National Security Council Interagency Policy Committee (IPC) Working Group on cybersecurity education and workforce issues and will continue to do so throughout the competency model development process. Because cybersecurity work is performed in many different positions and places throughout the Federal Government, it is not easy to identify them by looking solely at job titles or organization charts. For this reason, please provide us with documents such as position descriptions, vacancy announcements, crediting plans, training plans, performance management plans and any studies or competency models of cybersecurity work in your agency. We are also looking for information on your recruitment efforts, challenges and outcomes.

Because there are many types of cybersecurity work, where possible, we will develop competency models using the categories outlined by the IPC Cybersecurity work group:

IT Infrastructure, Operations, Maintenance and Information Assurance: Personnel who have significant responsibilities for designing, developing, operating, or maintaining the security of Federal IT infrastructures, systems, applications and networks. Also includes individuals who have responsibility for maintaining the confidentiality, integrity, and availability of the information contained in and transmitted from those systems and networks.

Domestic Law Enforcement and Counterintelligence: Personnel who analyze cyber events and environments to investigate potential threats and individuals who participate in law enforcement, counterintelligence, and other types of investigatory activities involving IT systems, networks, and/or digital information/evidence.

Specialized Cybersecurity Operations: Personnel who are employed by departments and agencies that are engaged in highly specialized, and largely classified, cybersecurity operations focused on collection, exploitation and response.

Please provide the requested information along with an agency point of contact to competency@opm.gov by January 15, 2010. As we move forward, we will also ask for your assistance in identifying subject matter experts to review draft task and competency lists and to coordinating survey administration. We plan to survey the cybersecurity workforce in late spring 2010.

Your assistance is greatly appreciated. If you have any questions about cybersecurity competencies, please contact Tara Ricci or Andrea Bright, respectively, at (202) 606-3600, or email tara.ricci@opm.gov or andrea.bright@opm.gov.

cc: Human Resources Directors