UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

Thursday, February 27, 2020

**MEMORANDUM FOR: HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES**

FROM: DALE CABANISS, DIRECTOR

Subject: America's Cybersecurity Workforce Executive Order 13870 Cybersecurity Aptitude Assessment Identification

**Overview:**

The Executive Order on America's Cybersecurity Workforce, issued on May 2, 2019, supports building and sustaining a strong Federal cybersecurity workforce. The continued effort to enhance the skills of the Federal cyber workforce is of national importance. This workforce protects data, systems, and operations vital to serving the American public, and defends our Nation against cybersecurity threats that impact the Federal Government's missions and the common good.

The Executive Order directed the U.S. Office of Personnel Management (OPM), U.S. Department of Commerce's (DOC) National Initiative for Cybersecurity Education (NICE), and the U.S. Department of Homeland Security (DHS) to identify and deliver a list of cybersecurity aptitude assessments for agencies to use in identifying current employees with the potential to acquire cybersecurity skills. As appropriate and consistent with law, agencies are directed to incorporate one or more of these assessments into their personnel development programs.

OPM convened an interagency group of subject matter experts from DOC, DHS and U.S. Department of Justice, Federal Bureau of Investigation. The interagency group reviewed research and conducted a data call to Federal agencies to learn which cybersecurity aptitude assessment(s) are currently being used across the Federal government for the purpose of reskilling. The group's findings are below.

**Assessments - Purpose and Types:**

Assessments can be used for the reskilling of current employees or to recruit and hire new talent. Utilizing assessments ensures the right talent is in the right place at the right time.

OPM recently issued a memorandum, Improving Federal Hiring through the Use of Effective Assessment Strategies to Advance Mission Outcomes. The memorandum provides guidance to enable simple and strategic hiring by: 1) analyzing and improving methods of assessing applicant quality; 2) involving subject matter experts in the assessment process; and 3) applying more rigor in determining minimum qualifications.

In contrast to a hiring assessment, the Executive Order is focused on aptitude assessments. In the context of this Executive Order, a cybersecurity aptitude assessment can be defined as any instrument or tool used for differentiation and prediction of current employees' abilities or skills (more broadly competencies) to perform cybersecurity work. Aptitude assessment examples may include coding challenges, work samples, computerized adaptive testing, and similar types of testing. Such assessments may be used to identify employees for cybersecurity training. In the Federal Government, aptitude assessments were recently used for the Cybersecurity Reskilling Academy pilot, as well as the code challenge pilot which was used to recruit new talent to the Federal government.

As agencies design their assessment strategies, they should consider the various types of assessments that are appropriate for assessing cybersecurity competencies.

- Cognitive Ability tests assess abilities involved in thinking (e.g., reasoning, perception, memory, verbal and mathematical ability, and problem solving). Such tests pose questions designed to estimate applicants' potential to use mental processes to solve work-related problems or to acquire new job knowledge.
- Structured Interviews are one of the most widely used methods of assessing job applicants. Due to its popularity, a great deal of research on improving the reliability and validity of the interview has been conducted. This body of research has demonstrated that structured interviews, which employ rules for eliciting, observing, and evaluating responses, increase interviewers' agreement on their overall evaluations by limiting the amount of discretion an interviewer is allowed.
- Biodata Test items are developed through behavioral examples provided by subject matter experts (SMEs). Biodata measures are based on the measurement principle of behavioral consistency, that is, past behavior is the best predictor of future behavior. Biodata measures include items about past events and behaviors reflecting personality attributes, attitudes, experiences, interests, skills and abilities validated as predictors of overall performance for a given occupation.
- Situational Judgment Tests (SJTs) present applicants with a description of a work problem or critical situation related to the job they are applying for and ask them to identify how they would handle it. Because applicants are not placed in a simulated work setting and are not asked to perform the task or behavior (as would be the case in an assessment center or a work sample), SJTs are classified as low-fidelity simulations.
- Personality Tests are designed to systematically elicit information about a person's motivations, preferences, interests, emotional make-up, and style of interacting with people and situations. Personality measures can be in the form of interviews, in-basket exercises, observer ratings, or self-report inventories (i.e., questionnaires).
- Training & Experience Point Method, sometimes called a crediting plan or rating schedule, is a systematic method used to assess previous experience, education, and training information provided by job applicants. These assessment factors are based on critical job requirements and competencies identified through a job analysis.

For more information about these types of assessments, please visit: https://www.opm.gov/policy-data-oversight/assessment-and-selection/other-assessment-methods/.

**Data Call Findings:**

To determine if and which aptitude assessments are being used by agencies, OPM sent a data call to Chief Information Officers and Chief Human Capital Officers, as well as HR Directors and Industrial Organizational Psychologists across the Federal government. The data call received 110 responses, with 31 indicating they utilize cybersecurity assessments and 79 indicating they do not utilize assessments. Three agencies provided explanations for how they utilize assessments.

- A large agency utilizes various assessments for the selection of new employees. This agency uses bio data, a work sample, structured interview, and assessments offered through USAHire to measure critical thinking, communication (written and oral), problem solving, and team building, etc. These skills are measured because they are related to success in the position. This agency uses these types of assessments to select talent for the following occupations: Computer Engineering Series, 0854; Electrical Engineering Series, 0855; Information Technology (IT) Management Series, 2210 (cyber); IT Management Series, 2210 (non-cyber); Telecommunications Series, 0391; (Non) IT Management Series, 2210 (cyber); (Non) IT Management Series, 2210 (non-cyber).
- A mid-sized agency is not using a formal assessment to evaluate Cybersecurity or IT applicants, but they are putting in place an assessment to evaluate their personnel for potential reskilling opportunities in Cybersecurity or IT occupations.
- An unnamed agency is utilizing cybersecurity assessments for reskilling current employees and selection of new talent. However, the unnamed agency did not provide additional details.

In addition, the U.S. Department of Defense (DoD) uses various assessments to predict success in cyber specialties. Assessment types include: cognitive ability tests, knowledge tests, personality assessments, and interest inventories. Additionally, the Military Services are continuously evaluating new types of assessments that can provide added information in predicting cyber training success. Specific examples include:

- Armed Services Vocational Aptitude Battery (ASVAB) - A multiple-aptitude battery that measures developed abilities and aptitude and helps predict future academic and occupational success in the military. Tailored ASVAB composites are used to assign recruits to military specialties.
- Cyber Test (CT) - A specialized knowledge test administered by all the Services for classification/assignment into cyber occupations/career fields. The CT assessment is used in combination with the ASVAB to enhance success in training. The test was developed to specifically predict performance in cyber-related training. The test includes items to assess knowledge and ability across four dimensions: Computer Operations, Networking and Communications, Security and Compliance, and Software Programming and Web Design.
- Electronic Data Processing Test (EDPT) - An aptitude test designed after the IBM Programmer Aptitude Test (IBM PAT). It is used exclusively by the United States Air Force for computer programming and cyber-related enlisted occupational specialties. The

EDPT components include: Arithmetic Reasoning, Number Series, Verbal Analogies, and Figure Analogies.

In 2015, the U.S. Air Force commissioned the University of Maryland *Center for Advanced Study of Language (CASL)* to conduct a two-year study to develop The Air Force Cyber Aptitude and Talent Assessment (AF-CATA). The main assessment goal is to enable decision makers to identify candidates who are cognitively equipped to succeed in cybersecurity, determine what position each candidate is best suited for and suggest training to broaden their knowledge base and strengthen their cyber skills. By assessing abilities rather than knowledge, the Air Force can broaden their cyber pipeline while improving outcomes and maintaining a highly skilled workforce. The Air Force is beginning to evaluate incremental prediction of CATA above operational assessments.

**Recommendations:**

Federal subject matter experts recommend the Federal government pursue a whole person approach for cybersecurity aptitude assessment for reskilling and the selection of new talent. The whole person approach should incorporate a mix of assessments that evaluate both cognitive and interpersonal competencies, as well as technical cybersecurity related knowledge, skills, and abilities. The decisions on what type of assessment to use should be guided by rigorous job analysis information and aligned with the outcome. Agencies should recognize that different approaches may be needed for different scenarios. For more information on cybersecurity aptitude assessments and types of cybersecurity assessments, please visit: https://community.max.gov/display/HumanCapital/Cybersecurity+Max+Page.

**Closing/Points of Contact:**

Thank you for your continued effort to build and sustain a strong Federal cybersecurity workforce. If there are any questions about cybersecurity assessments, please contact Kimberly Holden at (202) 606-8097 or kimberly.holden@opm.gov or Assessment_Information@opm.gov.

Attachment: Appendix 1: Cybersecurity Assessments – Tools & Resources (available on https://community.max.gov/display/HumanCapital/Cybersecurity+Max+Page)