UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Employee Services

April 11, 2022

Memorandum for Human Resources Directors

From: Robert H. Shriver, III
Associate Director
Employee Services

Subject: Cybersecurity Workforce Management Updates and Resources

I am pleased to share updates and resources to assist as you continue to manage and strengthen the skills of the Federal cybersecurity workforce across the Nation. In this memo, we highlight three updates with accompanying helpful resources.

Cybersecurity Position-Coding

First, we have updates that relate to requirements in the Federal Cybersecurity Workforce Assessment Act of 2015 and supplement guidance we initially issued in January 2017 concerning how to identify and code positions involved in cybersecurity, information technology, and cyber-related functions. These updates, contained in the attachment, elaborate on information learned over the last few years and introduce a new MAX page that centralizes relevant cybersecurity position-coding resources and agency best practices. We appreciate the feedback received from your agency representatives as we collaborated in gathering these updates and resources.

Cybersecurity JOA Tagging

Second, we call your attention to the work of an inter-agency pilot aiming to increase the visibility and effectiveness of our Federal cybersecurity job opportunity announcements (JOAs). Among other potential outcomes of this pilot is the enhanced ability to attract specifically needed cybersecurity skills rather than more generic GS-2210 skills typically advertised in our Federal JOAs. Read more on our MAX page (i.e., the first item in the "Best Practices" box) about the pilot, the benefits of JOA tagging, and how your agency can begin using a similar approach to advertising for cybersecurity talent.

Cybersecurity Hiring Resource Hub

Third, we introduce you to a new "Cybersecurity Hiring Resource Hub" on OPM's Future of Work website. The Resource Hub gives you easy access to resources, including information on flexibilities for recruiting, hiring, and retaining cybersecurity employees. Additionally, the attached 2-page information sheet elaborates on these flexibilities.

If you have questions about the updates described in this memo, please email them to CyberHRStrategy@opm.gov.

Attachments

cc: Chief Human Capital Officers, Deputy Chief Human Capital Officers, Chief Information Officers Council

OPM Memo: Cybersecurity Workforce Management Updates and Resources Attachment 1

Cybersecurity Position-Coding Updates and Resources
April 2022

1. MAX Page for Centralized Collection of Guidance and Resources

a. Cybersecurity position-coding guidance and other pertinent resources from the inter-agency community, including best practices, are available on a new MAX page.

2. Workforce Framework for Cybersecurity (NICE Framework)

a. The NICE Framework and its Work Roles are foundational to the cybersecurity position codes because the codes align to each of the Work Roles. NICE periodically revises its Framework to keep it updated. Current and previous versions of the Framework are available on the NICE website; future versions will also be posted there.

b. Work Roles presented in future versions of the NICE Framework may evolve and change in number, but agencies may use, or code their positions to, current or previous Work Roles in perpetuity.

c. The NICE Framework Categories arrange Work Roles into groupings. These groupings are useful for educating managers and human resources staff on the applicability of the NICE Framework to coding their agency workforce. Other interpretations of Work Role groupings are available on the MAX page.

3. Conditional Criteria Associated with Cybersecurity Position-Coding

a. Certain cyberspace effects and intelligence-related functions are typically performed in organizations with particular authorities under title 10, 50, 32, etc., of the US Code, rather than organizations with title 5 authorities. The NICE Framework Categories of "Collect and Operate" (sometimes referred to as cyberspace effects) and "Analyze" (intelligence-related) contain these Work Roles. Other interpretations of Work Roles assigned to these functions are available on the MAX page.

b. During GAO's audit of agencies' implementation of Federal Cybersecurity Workforce Assessment Act requirements, it directed agencies to assign a Work Role code other than "000" to each position classified in the GS-2210 occupational series. Although not a rule from OPM, GAO believes this is consistent with the intent of the Act.

c. Agencies may want to tailor their internal systems to operate according to the conditions listed above. For example, to improve cybersecurity position-coding accuracy, agencies could program internal systems to restrict use of Work Role codes that are inappropriate for their circumstances.

Federal IT/Cybersecurity: Governmentwide Recruitment and Retention Authorities

Time is of the essence – the Federal Government must close the skills gap and hire IT/Cyber talent to strengthen our cyber defense. ***Consider the available authorities and incentives to modernize IT and build a workforce of the 21st century.***

Hire IT/Cyber Talent Fast

Use the Direct Hire Authority (DHA)

A DHA is an appointing (hiring) authority that the Office of Personnel Management (OPM) can provide to Federal agencies for filling vacancies when a critical hiring need or sever shortage of candidates exists.

Which cybersecurity/IT federal positions are covered by DHA?

These occupational series are covered at grade levels 12-15:

GS-0854	**Computer Engineers (Cybersecurity)**
GS-1550	**Computer Scientists (Cybersecurity)**
GS-0855	**Electronics Engineers (Cybersecurity)**
GS-2210	**IT Cybersecurity Specialist**

Read the CHCOC announcement for more information.

Ways to Recruit Senior Executive Service (SES)

Use one of the following authorities to hire an executive to lead America's workforce.

Noncompetitive Appointment or Reinstatement occurs when a SES Candidate Development Program graduate is certified by the Qualifications Review Board, or a former SES member is eligible for reinstatement. *(5 CFR 412 subpart C)*

Noncareer Appointment occurs when an agency makes a SES noncareer appointment to SES positions after OPM authorization for each appointment. *(5 CFR 317 subpart F)*

Reassignment or Transfer occurs when a career SES is voluntarily reassigned within their agency or transferred to another agency to any SES position for which they are qualified. *(5 CFR 317 subparts G and I)*

Limited Term Appointment occurs when a non-Federal Intergovernmental Personnel Act assignee is appointed to an SES position with prior OPM authorization. *(5 U.S.C. 3371-3375, and 5 CFR part 334)*

Current Student or Recent Graduate

Looking for a student or recent graduate with a degree in a cybersecurity related field?

Pathways Program provides ways for agencies to recruit and hire students and recent graduates for jobs and internships.

- Presidential Management Fellows (PMF) Program is a Pathways program and the Federal Government's premier leadership development program for advanced degree (e.g., masters or professional degree) candidates. It is a highly selective, two-year fellowship and leadership development program that recruits recent graduates and current graduates.
- Cyber Corps®: Scholarship for Service (SFS) Program is a governmentwide program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. It provides scholarships to cybersecurity students in exchange for government service upon graduation.

Bring in a Consultant or Detail – Discover a fresh approach!

Experts and Consultants Appointments to perform temporary or intermittent expert or consultant work; paid up to GS-15, Step 10, base rate (or higher rate under agency-specific authority). *(5 U.S.C. 3109, and 5 CFR part 304)*

Details Within and Between Agencies for up to 120 days. *(5 U.S.C. 3341, 5 CFR part 300 subpart C; 31 U.S.C. 1535. See also 64 Comp. Gen. 370.)*

Visit CyberCareers.gov for resources on how to recruit, hire, and retain IT/Cyber talent!

Federal IT/Cybersecurity: Governmentwide Recruitment and Retention Authorities

Time is of the essence – the Federal Government must close the skills gap and hire IT/Cyber talent to strengthen our cyber defense. ***Consider the available authorities and incentives to modernize IT and build a workforce of the 21st century.***

Incentives: Your agency can offer financial incentives as a way to recruit and retain talent!

Recruitment Incentive offers newly appointed employees in difficult-to-fill positions up to 25 percent of basic pay multiplied by the number of years in the service agreement (up to 4 years). *(5 U.S.C. 5753 and 5 CFR part 575, subpart A)*

Relocation Incentive offers current employees who must relocate to difficult-to-fill positions up to 25 percent of basic pay multiplied by the number of years in the service agreement (up to 4 years). *(5 U.S.C. 5753 and 5 CFR part 575, subpart B)*

Retention Incentive offers highly-qualified employees or employees filling a special agency need that are likely to leave the Federal service up to 25 percent of basic pay for an individual or 10 percent for a group. *(5 U.S.C. 5754 and 5 CFR part 575, subpart C)*

Student Loan Repayment Program permits agencies to repay Federally insured student loans as a recruitment or retention incentive for candidates or current employees of the agency of up to a maximum of $10,000 for an employee in a calendar year and a total of not more than $60,000 for any one employee. (*5 U.S.C. 5379 and 5 CFR part 537*)

Pay Flexibilities

Your agency can offer more money based on occupation and skill

Governmentwide Special Rates are available for certain entry and developmental computer engineers, computer science specialists, and information technology (IT) management specialists. Agencies may request OPM approval of increased or new special rates to address staffing needs. *(5 U.S.C. 5305 and 5 CFR part 530, subpart C)*

Critical Position Pay may be approved by OPM, in consultation with OMB, so that an agency may fix the rate of basic pay for one or more positions requiring an extremely high level of expertise at a higher rate than would otherwise be payable for the position, up to level I of the Executive Schedule. (5 U.S.C. 5377 and 5 CFR part 535)

Superior Qualifications and Special Needs Pay-Setting Authority permits agencies to set a new General Schedule (GS) employee's pay above step 1 (up to step 10), because of the employee's superior qualifications or the agency's special need of the candidate's services. *(5 CFR 531.212)*

Maximum Payable Rate Rule permits agencies to set pay at a higher than normal GS rate based on a higher rate of pay the employee previously received in another Federal job (not to exceed step 10). *(5 CFR 531.221-223)*

Visit OPM's Flexibilities for Recruitment and Retention page for more information.

Leave Flexibilities

Your agency can grant additional leave accrual

Creditable Service for Annual Leave Accrual for Non-Federal Work Experience and Experience in the Uniformed Service permits agencies to grant service credit for certain non-Federal or uniformed service experience that otherwise would not be creditable for determining the annual leave accrual rate for newly appointed or reappointed employees or military retirees. *(5 U.S.C. 6303(e) and 5 CFR 630.205)*

Read the fact sheet for more information.

There is also a Pay and Leave Flexibilities course available on OPM's website.

Visit CyberCareers.gov for resources on how to recruit, hire, and retain IT/Cyber talent!