TECH WORKFORCE IDENTIFICATION AND CODING

1. **REASON FOR ISSUE:** This handbook establishes roles and responsibilities for identifying Information Technology (IT), Cybersecurity and Cross-functional positions, aligning work roles and assigning corresponding work role codes to identified positions; contains information on the structure and core elements of work roles; and provides the Department of Veteran Affairs (VA) specific guidance for the identification, alignment and coding of these work roles.

2. **SUMMARY OF CONTENT/MAJOR CHANGES:** This handbook establishes guidance on the standards and requirements for identifying IT, Cybersecurity and Cross-functional positions, aligning work roles and assigning work role codes to identified positions. It incorporates requirements from the Federal Cyber Workforce Assessment Act (FCWAA) and the Office of Personnel Management (OPM) January 4, 2017, memorandum, “Guidance for Assigning New Cyber Codes to Positions with Information Technology (IT), Cybersecurity, and Cyber-Related Functions.” Although Federal Cybersecurity Workforce Assessment Act (FCWAA) and OPM guidance include “cybersecurity” in their titles, the wording within the FCWAA and OPM guidance requires that all IT, Cybersecurity and Cyber-related (or cross-functional) positions be aligned to at least one work role, as reflected in this guide.

3. **RESPONSIBLE OFFICE:** Office Information and Technology and Chief Information Office (OIT) (005).

4. **RELATED DIRECTIVES AND HANDBOOK:** VA Directive 6505: VA Cyber Workforce Management, dated January 25, 2022, VA Directive 6500: VA Cybersecurity Program, dated February 24, 2021, VA Handbook 6500: Risk Management Framework for VA Information Systems – VA Information Security (INFOSEC) Program, dated February 24, 2021, and VA Handbook 5003: Position Classification and Position Management Part 1, dated August 22, 2022.

5. **RESCISSION:** Not applicable.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information and Technology
Chief Information Officer

DISTRIBUTION: Electronic Only

TECH WORKFORCE IDENTIFICATION AND CODING
TABLE OF CONTENTS

TECH WORKFORCE IDENTIFICATION AND CODING

1. PURPOSE.

a. The VA tech workforce must continue to advance to address constantly evolving security threats while meeting the Department's mission requirements. This requires policies and processes which reflect the Department's understanding that the Department of Veteran Affairs (VA) tech workforce extends beyond the Office of Information and Technology (OIT). Although VA has completed and submitted its initial work role alignment to the Office of Personnel Management (OPM) for its positions identified within the tech workforce, the need for review and validation of tech positions will be required as work and roles evolve based on a changing tech landscape. This varied workforce includes personnel who build, secure, operate, defend and protect VA's data and resources.

b. VA will standardize identifying positions involved in the execution of IT, Cybersecurity and Cyber-related work, aligning work roles to positions and assigning corresponding work role codes to positions by leveraging lexicons such as the National Initiative for Cybersecurity Education (NICE) Framework and the Department of Defense (DOD) Cyber Workforce Framework in conjunction with OPM cyber coding guidance. This standardization will provide the Department a clear understanding of the composition of skills in the current tech workforce. These frameworks serve as lexicons to clearly define and identify the tech workforce using work roles that describe the baseline skills/functional work, aligned tasks and aligned knowledge and skills required to perform those tasks. Identifying the tech population using common, standardized terms and definitions will enable the development of capabilities that aid the recruitment, retention, training and qualifications of the VA tech workforce.

c. This handbook incorporates requirements from the Federal Cyber Workforce Assessment Act (FCWAA) of 2015 contained in P.L. 114-113, and OPM's January 4, 2017 memorandum, "Guidance for Assigning New Cyber Codes to Positions with Information Technology (IT), Cybersecurity and Cyber-Related Functions." Although FCWAA and OPM guidance include "cybersecurity" in their titles, the wording within the FCWAA and OPM guidance requires that all IT, cybersecurity and cyber-related positions be aligned to at least one work role, as reflected in this guide.

2. SCOPE. This handbook applies to all VA employees and leadership aligned to IT, Cybersecurity and Cyber-related work roles as aligned with OPM guidance.

3. RESPONSIBILITIES. An enterprise-wide effort to identify tech positions, align tech work roles and assign work role codes to VA tech positions (filled and vacant) needs broad stakeholder participation.

a. **Assistant Secretary for OIT /Chief Information Officer (CIO).** VA CIO shall:

(1) Coordinate with VA Administrations and staff offices to implement program objectives to address identification, alignment, and coding of the VA tech positions to work roles.

(2) Provide analytical reports to VA stakeholders and coordinate with Chief Human Capital Officer (CHCO) to distribute reports to OPM.

(3) Provide oversight and analysis of identified tech positions.

b. **Under Secretaries, Assistant Secretaries and Other Key Officials** shall:

(1) Coordinate with the Office of People Science (OPS) to implement program objectives for addressing the identification, alignment and coding of VA tech positions to work roles.

c. **Chief Human Capital Officer (CHCO)** shall:

(1) Ensure required coding data elements are integrated into VA's Human Resources (HR) system of record.

(2) Develop formalized processes and procedures for HR personnel executing tech coding requirements.

(3) Provide identification and coding data (e.g. reports) to VA stakeholders and coordinate with the Director of People Readiness and CIO when distributing reports to OPM.

(4) Ensure work role(s) and associated codes are integrated into position description that require the performance of tech work.

(5) Support the modification of position descriptions to accurately reflect the duties of tech positions.

d. **OIT, Office of People Science** shall:

(1) Provide implementation guidance for VA administration and staff offices to:

(a) Set milestones and monitor progress.

(b) Coordinate with CHCO to develop functional requirements for modifying HR systems of record to support coding, analysis and reporting of the tech workforce.

(c) Identify, define and provide required coding data elements to VA CHCO for integration into HR systems of record.

(d) Support accurate application of work roles, coding, reporting and analysis of VA tech positions.

(e) Provide assistance and training (e.g. in-person or virtual) to administrations, staff offices and supervisors for work role alignment.

(f) Provide analytical reports to VA stakeholders and coordinate with the CHCO to distribute reports to OPM.

(g) Support integrated analysis of work roles and occupation series as they relate to mission critical occupations, work roles of critical need, strategic workforce planning, staffing analysis and manpower management.

(2) Perform OIT manpower management studies, workforce planning activities and position description generation to:

(a) Ensure work role(s) and associated code(s) are integrated into OIT position descriptions requiring the performance of tech work.

(b) Review OIT position descriptions to confirm work role(s) are accurately reflected within the major duties of tech positions.

(c) Audit OIT work role alignment, assessing it against mission and function and validating supervisors' and managers' input of assigned work role(s).

(d) Provide integrated analysis of OIT's work roles and occupation series as they relate to mission critical occupations, work roles of critical need, staffing planning and manpower management.

e. **All VA Supervisors and Managers with tech positions** shall:

(1) Socialize and communicate the requirement to identify, align and code work roles to all vacant and filled positions, as specified in this handbook and the guidance provided by OPS.

(2) Set milestones and monitor progress for the alignment of work roles and updating position descriptions.

(3) Evaluate position requirements and align appropriate work role(s) to positions.

(4) Integrate work role(s) and attributes into the major duties section of the position description.

4. PROCEDURES.

a. UNDERSTANDING THE TECH WORKFORCE.

(1) Defining the VA Tech Workforce.

(a) The VA tech workforce encompasses the skills required to build, secure, operate, defend and protect technology, data and resources; lead, acquire and manage tech initiatives; develop tech workforce talent; and conduct cyber-related legal and law enforcement activities. This definition is broad and reflects the wide-ranging performance of tech activities throughout VA. Below defines the three skills communities within the VA Tech Workforce: IT, Cybersecurity and Cross-Functional

(b) **IT Skills Community**- Skills required to design, build, configure, operate and maintain IT, networks and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate and dispose of IT and information resource management; and the management, storage, transmission and display of data and information.

(c) **Cybersecurity Skills Community**- Skills are required to secure, defend and preserve data, networks, net-centric capabilities and other designated systems by ensuring appropriate security controls and measures, and taking internal defense actions. This includes access to system controls, monitoring, administration and integration of cyber into all aspects of engineering and acquisition of cyber capabilities.

(d) **Cross-Functional Skills Community**- Skills needed to lead, acquire and manage tech initiatives; develop tech workforce talent; and conduct tech-related legal and law enforcement activities.

b. IDENTIFYING TECH POSITIONS.

(1) A general guideline is that any position performing functions within the IT, Cybersecurity or Cross-Functional skills communities are considered tech. Those occupation series noted as core cyber in Appendix A should have an active cyber work role and code assigned. This is inclusive of all positions within the 2210 occupation series. Additionally, any position that was filled using a direct hiring authority for IT, Cybersecurity or Cross-Functional skills will also be considered a tech position. This excludes what are commonly referred to as cyber citizen positions, defined as general users of technology to carry out their day-to-day activities. In our current connected world, almost all VA employees meet this definition to some extent. Those in cyber citizen positions use IT systems and products as tools to complete their actual tasks and responsibilities versus being

directly involved in developing, delivering or supporting IT systems and services.

(2) Work roles are not occupation series-specific and may align to more than one OPM occupation series. For example, the Systems Requirement Planner work role 641 could apply to positions in several occupation series such as 2210 IT Management, 0391 Telecommunications, 0301 Miscellaneous Administration and Program, 0343 Management and Program Analysis, 0855 Electronics Engineering, 0854 Computer Engineering and 2003 Supply Program Management.

(3) Additionally, work roles can be applied from two different perspectives:

(a) Baseline skill requirements to execute the tasks as written or

(b) Baseline skill requirements to be employed for alternative purposes such as audit, compliance, inspections, oversight and so forth. While these guidelines provide a starting point for identifying tech positions, VA supervisors will review positions in the occupation series identified in Appendix A, as well as other relevant occupations, to determine if they perform tech work.

c. **ALIGNING WORK ROLES TO POSITIONS.**

(1) Choosing the Appropriate Work Role.

(a) The selection of one or more work roles is determined by reviewing the position description, then selecting the skills community and work role that best aligns with the primary function and baseline skills required for that position. Refer to the Work Role Tool User Guide for work role details.

(b) A single position can have work roles aligned from multiple skills communities.

(2) Primary and Additional Tech Work Role Differentiation.

(a) Per OPM guidance, any identified tech position may be aligned with no more than three work roles, a primary and up to two additional. The first work role is considered the primary work role and indicates that a substantial amount of time is spent performing the tasks of a work role or indicates the primary baseline skill required to perform the duties of the position. Additional work roles may be identified to capture other tech work or skills required for the position. For example, a position with the primary work role of Technical Support Specialist might also be assigned the additional work role of System Administrator. Both positions involve diagnosing, solving and triaging technical issues within an organization, but the System Administrator

performs these functions while also focusing on performance, security and efficiency of a system or a systems component. However, the selection of a single tech work role may provide enough information to ensure the right skill set is identified.

(3) Breadth and Depth Work Roles.

(a) There are two different types of work roles: breadth and depth. Breadth work roles are those that require knowledge of a range of skills at a high level, whereas depth work roles are those that require knowledge of a specific set of skills at an intimate level. All skill communities can contain depth and breadth work roles. Examples of each are listed here:

i Breadth roles:

(A) Software Developers (621).

(B) Systems Developers (632).

(C) Cyber Defense Analyst (511).

ii Depth roles:

(A) Research and Development Specialists (661).

(B) Systems Requirements Planner (641).

(C) Systems Test & Evaluation Specialists (671).

(D) Cyber Defense Incident Responder (531).

(E) Cyber Defense Infrastructure Support Specialist (521).

(4) Work Role Pairings.

Some work roles are more likely to be complemented by or paired with another work role. These work role pairings are typically based on mission-specific functions of a position, technical specificity required for a position, or specific capabilities needed for a position. Examples include, but are not limited to:

(a) Cyber Defense Analyst may be paired with a Cyber Defense Incident Responder or another work role supporting mission requirement.

(b) Systems Developer or Software Developer may be paired with an area of technical expertise, such as a System Testing and Evaluation Specialist or Research and Development Specialist.

(c) Software and/or Systems Developer may be paired with Data Analyst for capabilities related to data science.

(d) Cyber Instructor paired with one or more work roles highlighting the area(s) of expertise required to teach the coursework.

(e) Instructional Curriculum Developer paired with one or more work roles highlighting the area(s)of expertise required to develop the curriculum.

(5) Work Roles and Position Descriptions.

Integrate attributes of aligned cyber work role(s) and associated codes into new and updated position descriptions by:

(a) Selecting the appropriate tasks, knowledge and skill statements for each work role aligned.

(b) Incorporating work role name, description and tasks into the major duties section of the position description.

(c) Prioritizing the work roles, if more than one work role is identified, with the highest priority work role identified as “Primary”.

(d) Including the knowledge and skill statements of the selected work roles into “Factor 1: Knowledge Requirements” along with any other position specific knowledge and skill requirements.

d. **ASSIGNING WORK ROLE CODES TO POSITIONS.**

(1) Once a position has been aligned to one or more work role, the appropriate work role code(s) can be applied. OPM’s Cyber Coding Guidance Memo provides a three-digit numerical identifier (or work role code) for each work role. All identified tech positions will be coded with at least one work role code. Only those positions that perform substantial work involving IT, cybersecurity or cyber-related work (see Section 3.1) receive a work role code(s). No action is required by supervisors for non-cyber positions.

(a) Work Role Tool User Guide displays a listing of the OPM Cyber Codes assigned to the work roles.

(b) **Use of Primary and Additional Work Role Codes.** While up to three work role codes can be assigned, it is not required to assign more work role codes than are appropriate. Work role codes should be applied in priority order, based on the duties of the position and skills required for the position as aligned to each corresponding primary and additional work role identified in paragraph 4(c). When only one work role (primary) has been aligned to a position, this

typically indicates a performance percentage of 50% or greater of time is spent in the respective work role, and only one work role code will be assigned.

i For example, if the position has only been aligned to the Cyber Defense Analyst work role (511), it will be coded as follows: Position A: 511

ii If both primary and additional work roles (second and third, respectively) were identified for a position (see para 4(c)), then the corresponding work role codes in accordance with OPM Guidance should be assigned to that position based upon the prioritization. For example, a position aligned to a primary work role of Cyber Defense Analyst (511) and a single additional work role of Cyber Defense Incident Responder (531) will be coded as follows: Position B: 511 531

iii A position aligned to a primary work role of Cyber Defense Analyst (511), with two additional work roles of Cyber Defense Incident Responder (531), and Vulnerability Assessment Analyst (541) will be coded in prioritized order as follows: Position C: 511 531 541.

(2) Update position data to include work roles.

(a) Integrate the attributes of aligned cyber work role(s) and associated codes into new and updated position descriptions.

(b) Identify codes on OPM's official forms (for example, OF-8).

(c) Work with HR to ensure the update to HR system(s) of record.

5. REFERENCES.

a. Federal Cybersecurity Workforce Assessment Act of P.L. 113-114 (pages 735 - 737)

b. Description of Work Roles and 3-Digit Cybersecurity Codes (within the Federal Cybersecurity Coding Structure, Table 1, Pages 4-11)

c. DoD Cyber Workforce Framework

d. NICE Cybersecurity Workforce Framework

e. National Initiative for Cybersecurity Careers and Studies

f. OPM 2017 Memo - Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions

g. OPM CHCO Council Memo – Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need

h. Work Role Tool User Guide

APPENDIX A – Occupation Series Alignment to Tech Work

Table 2 provides a listing of occupation series, in consideration with OPM Guidance Memo. It is not meant to be all-inclusive but may provide a starting point for analyzing and aligning work roles to tech positions. The act of coding VA positions will provide new data to continue to refine this table. This list is a representative group of occupations.

Table 2: Tech Related Occupation Series

Core	A core tech occupation means that every position within the occupation is considered tech.
0332	Computer Operation
0335	Computer Clerk and Assistant
0390	Telecommunications Processing
0391	Telecommunication
1550	Computer Science
2210	IT Management
2299	IT Management Student Trainee
2502	Telecommunications Mechanic
Tier 1 – Strong Relationship	Tier 1 occupations have a strong alignment with tech. Many typical occupations are in engineering disciplines.
0132	Intelligence Research
0850	Electrical Engineering
0854	Computer Engineering
0855	Electronics Engineering
0856	Electronics Technical
1601	Biomedical Technician
0858	Biomedical Engineer
Tier 2 – Some Tech Roles	Tier 2 occupations have some positions with a tech focus. Those positions may fulfill a need for specific, recognized tech expertise within a certain occupation.
0080	Security Administration
0201	Human Resources
0306	Government Information
0308	Records and Information Management
0394	Communications Clerical
0501	Financial Administration and Program
0511	Auditing
0801	General Engineering
0830	Mechanical Engineering
0905	General Attorney
1102	Contracting
1410	Librarian

1411	Library Technician
1412	Technical Information Services
1420	Archivist
1421	Archives Technician
1499	Library and Archives Student Trainee
1510	Actuary
1515	Operations Research
1520	Mathematics
1530	Statistician
1801	General Inspection, Investigation, Enforcement and Compliance
1811	Criminal Investigation
Tier 3 –May Have Tech Roles	These types of occupations have positions located in many organizations and on many staffs. The work of these occupations is not inherently tech, but the positions may be located within an organization with a tech-related mission. Or the occupation may have been selected because there was no applicable occupation series. Without a tech work role or code, there would be very little ability to identify these positions as tech.
0301	Miscellaneous Administration and Program
0303	Miscellaneous Clerk and Assistant
0340	Program Management
0343	Management and Program Analysis
0346	Logistics Management
1101	General Business and Industry
1701	General Education and Training
1712	Training Instruction
4701	Miscellaneous General Maintenance and Operations Work

APPENDIX B – Requirements and Limitations for Application of Tech Work Roles

1. To be used **ONLY in VA OIS CSOC**:
    a. Cyber Defense Analyst (511)
    b. Cyber Defense Forensics Analyst (212)
    c. Cyber Defense Incident Responder (531)
    d. Cyber Defense Infrastructure Support Specialist (521)
    e. All Source Intelligence Analyst/Cyber Intelligence Analyst (111)
2. For defensive purposes **ONLY in VA OIS Security Assessment and Validation Directorate (SAVD)**:
    a. Cyber Operations Planner (332)
    b. Exploitation Analyst (121)
3. To be used **ONLY in OIS CSOC or SAVD**:
    a. Vulnerability Assessment Analyst (541)
    b. Threat/Warning Analyst (141)
4. Tech Work Roles NOT to be used at VA, in accordance with Title 10, United States Code, Title 32, United States Code, and Title 50, United States Code:
    a. Intelligence Community work roles which **REQUIRE Title 50, United States Code (U.S.C) Authority**:
        (1) All Source Collection Manager (311)
        (2) All Source Collection Requirements Manager (312)
        (3) Cyber Intelligence Planner (331)
        (4) Multi-Disciplined Language Analyst (151)
5. Cyber Effects Community work roles which REQUIRE Title 10 U.S.C /Title 32 U.S.C /Title 50 U.S.C Authorities:
    a. Cyber Operator (321)
    b. Partner Integration Planner (333)
    c. Mission Assessment Specialist (112)

d. Target Network Analyst (132)

e. Target Developer (131)

6. Additional Work Role Requirements and Limitations:

a. Authorizing Official (611) – REQUIRES CIO Appointment/Designation Letter.

b. Cyber Policy & Strategy Planner (752) – Applies to both Policy, Strategy and NON-SES Leadership positions.

c. Executive Cyber Leadership (901) – SES Only Cyber Leadership positions.

APPENDIX C – VA Tech Work Role FAQs

The Federal Cybersecurity Workforce Assessment Act (FCWAA) of P. L. 113-246 requires the identification and coding of all tech positions across the government. Initial coding was due in April 2018; however, all Departments must continuously code new positions and validate existing coding to ensure compliance with the mandate. At the VA, the Office of Information Technology (OIT), in collaboration with the Office of Human Resources and Administration (HRA), leads this effort and guides the Administrations in appropriately identification and coding their positions.

Q: What are the FCWAA's coding requirements?
A: The Federal Government must align work roles to all filled and vacant Information Technology, Cybersecurity, and Cyber- related positions. Each position must be coded using guidance from Office of Personnel Management (OPM).

Q: What is a tech position?
A: Tech positions are identified based on the functional work of the position or baseline skills required to perform in the position. Tech positions may require Information Technology, Cybersecurity, or Cross-Functional skills.

Q: What are work roles?
A: Work roles are additional descriptors applied in conjunction with OPM occupation series. Work Roles are not occupation series-specific and may align to more than one occupation series (e.g., 2210, 0332, 0390, 2502). There are 52 total work roles, 43 of which are applicable to VA. Codes were created by OPM as numerical representation of the work roles for systems of record and reporting.

Q: Are there different ways to apply work roles and codes?
A: Work Roles can be applied from two different perspectives:

1. Baseline skill requirements to execute the tasks as written, or
2. Baseline skill requirements to be employed for alternative purposes, including audit, compliance, inspections, oversight, etc.

Q: What is the difference breadth and depth work roles?
A: There are two types of work roles– breadth and depth. Breadth work roles require knowledge of a range of skills at a high level (e.g., Software Developers, Systems Developers, and Cyber Defense Analysts). Depth work roles require knowledge of a specific set of skills at an intimate level (e.g., Research & Development Specialists, System Requirements Planners, and Systems Test & Evaluation Specialists, Cyber Defense Incident Responder, and Cyber Defense Infrastructure Support Specialist).

Q: Who can I contact for additional information?
A: People Readiness team at VAOITPeopleReadiness@va.gov.