**Department of Veterans Affairs**
**Washington, DC 20420**

**VA DIRECTIVE 6505**
**Transmittal Sheet**
**January 25, 2022**

# VA CYBER WORKFORCE MANAGEMENT

1. **REASON FOR ISSUE:** To establish policies and assigned responsibilities for managing, maintaining and supporting the VA cyber workforce, consistent with VA strategies.

2. **SUMMARY OF CONTENTS:**

   a. Defines the cyber workforce, establishes a Cyber Workforce Management Office, formalizes the Cyber Workforce Management Program and authorizes establishment of a Cyber Workforce Management Committee (CWMC) to govern and monitor the health and welfare of the VA cyber workforce. The CWMC will be compromised of various VA stakeholders toensure that the requirements of this directive and subsequent handbooks are met.

   b. Unifies the overall VA cyber workforce which is comprised of two core workforce skills communities (Information Technology (IT) and Cybersecurity) and four cross functional skills communities (Lifecycle Management, Talent Management, Strategic Management and Legal/Law Enforcement) to align, manage and standardize employment of cyber work roles, identify cyber positions and establish baseline technical qualifications requirements.

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

4. **RELATED DIRECTIVE AND HANDBOOK:** VA Directive 6500: VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500: Risk Management Framework for VA Information Systems –VA Information Security Program (February 24, 2021).

5. **RESCISSION**: None.

**CERTIFIED BY**

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

**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**

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

**DISTRIBUTION**: Electronic only

# VA CYBER WORKFORCE MANAGEMENT PROGRAM

## 1. PURPOSE.

a. The purpose of the VA Cyber Workforce Management Program is to establish workforce management initiatives to improve recruitment, retention, development and growth opportunities for VA's cyber workforce.

The cyber workforce is occupation series agnostic and, as defined in this directive, is comprised of personnel who build, secure, operate, defend and protect technology, data and resources; lead, acquire and manage cyber initiatives; develop cyber workforce talent; and conduct cyber related legal and law enforcement activities. It is comprised of two primary skills communities of IT and Cybersecurity and four cross functional areas of Lifecycle Management, Talent Management, Strategic Management and Legal/Law Enforcement.

b. This directive:

(1) Authorizes establishment of a VA Cyber Workforce Management Committee (CWMC) to monitor the health and welfare of the VA cyber workforce and ensure that the requirements of this directive are met.

(2) Unifies the overall VA cyber workforce to align, manage and standardize employment of cyber work roles, identify cyber positions and establish baseline technical qualifications requirements.

(3) Aligns VA's cyber workforce with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, National Initiative of Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICEFramework).

## 2. POLICY.

a. It is VA policy that:

(1) VA Cyber Workforce Management Program will develop initiatives to identify, recruit, retain and enhance VA's cyber workforce; as well as promote growth and development of cyber knowledge, skills and abilities.

(2) VA will maintain a total workforce management perspective to provide qualified Federal cyber personnel to identified and authorized positions, augmented where appropriate by contracted services support. These personnel function as an integrated workforce with complementary skill sets to provide an agile, flexible response to VA requirements.

(3) Nothing in this directive replaces or infringes on the responsibilities, functions, or authorities of VA leadership as prescribed by law or Executive Order.

## 3. RESPONSIBILITIES.

a. **Assistant Secretary for Information and Technology and Chief Information Officer (A/S OIT/CIO),** shall:

(1) Establish the VA Cyber Workforce Management (CWM) Office to resource, manage and institute the CWM Program and Chair the Cyber Workforce Management Committee (CWMC)

(2) Direct CWM office to develop, manage and orchestrate the integration of cyber workforce management policies and capabilities that support identification and qualifications for the cyber workforce, in accordance with this directive.

(3) Coordinate with CWMC to ensure appropriate resources are allocated to the cyber workforce management program.

(4) Coordinate with CWMC for annual assessment of the Cyber Workforce Management Program.

b. **Under Secretaries, Assistant Secretaries and Other Key Officials,** shall ensure that positions performing cyber functions are identified with the Office of Personnel Management (OPM) cyber codes and personnel occupying cyber coded positions are qualified.

c. **Deputy Chief Information Officer (DCIO) for Information Security (OIS)** and **Chief Information Security Officer (CISO)**, under the authority and direction of the VA CIO, shall:

(1) Identify a representative to participate in the CWMC.

(2) Support the implementation of policy in support of the cyber workforce management program.

d. **Deputy Assistant Secretary (DAS) for Development Security Operations (DSO),** under the authority and direction of the VA CIO, shall:

(1) Identify a representative to participate in the CWMC.

(2) Support the implementation of policy in support of the cyber workforce management program.

e. **Deputy Chief Information Officer (DCIO) for IT Resource Management (ITRM),** shall:

(1) Identify a representative to participate in the CWMC.

(2) Collaborate with CWM to develop and integrate cyber workforce managementrequirements into existing ITRM functions and processes.

f. **Deputy Chief Information Officer (DCIO) for Office of Strategic Sourcing (OSS),** shall:

(1) Identify a representative to participate in the CWMC.

(2) In collaboration with the Office of Acquisition, Logistics and Construction (OALC), integrate policies established in this directive and supporting guidance into acquisition policy, regulations and documentation as applicable for contracted support services.

g. **Director, Cyber Workforce Management (CWM),** shall:

(1) Perform the duties as the chair of the CWMC and identify co-chair(s)

(2) Establish policies addressing cyber workforce identification and qualification standards and requirements.

(3) Oversee the development and maintenance of the cyber workforce qualification standards and requirements in accordance to this directive and other applicable references.

(4) Develop guidance regarding how cyber workforce related metrics are determined, established, defined, collected and reported.

(5) Manage and orchestrate the integration of cyber workforce management policies and capabilities with VA stakeholders.

h. **Assistant Secretary for Human Resources & Administration/Operations, Security and Preparedness (A/S HRA/OSP)**, in addition to the responsibilities listed above, shall identify a representative to participate in the CWMC.

**i. Principal Executive Director, Office of Acquisition, Logistics and Construction (OALC)**, in addition to the responsibilities listed above, shall collaborate with the Deputy Chief Information Officer (DCIO) for Office of Strategic Sourcing (OSS), to integrate policies established in this directive and supporting guidance into acquisition policy, regulations and documentation as applicable for contracted support services.

j. **Director, VHA/WMC/ HR Management and Consulting Service** shall identify as representative to participate as a stakeholder in the CWMC.

## 4. REFERENCES.

a. **Statutes and Regulations and National Institute of Standards and Technology (NIST)**

(1) 6 U.S. Code § 146, Federal Cybersecurity Workforce Assessment Act

(2) Executive Order No. 13870, 84 FR 20523, America's Cybersecurity Workforce, May 2, 2019

(3) Executive Order No. 13800, 82 FR 22391, Strengthening the Cybersecurity of Federal networks and Critical Infrastructure, May 11, 2017

(4) National Institute of Standards and Technology Special Publication 800-181, NICE Workforce Framework for Cybersecurity

**b. Office of Personnel and Management**

(1) OPM Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce, October 2018

(2) Memorandum: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity and Cyber-Related Functions, January 4, 2017

**c. VA Directives and Handbooks**

(1) VA Directive 6500: VA Cybersecurity Program

(2) VA Handbook 6500: Risk Management Framework for VA Information Systems - VA Information Security Program

## 5. DEFINITIONS.

a. **Cyber Workforce:** The cyber workforce is occupation series agnostic and, as defined in this directive, is comprised of personnel who build, secure, operate, defend and protect technology, data and resources; lead, acquire and manage cyber initiatives; develop cyber workforce talent; and conduct cyber related legal and law enforcement activities. SOURCE: National Initiative for Cybersecurity Career and Studies

b. **Cybersecurity Skills Community:** Skills needed to secure, defend and preserve data, networks, net-centric capabilities and other designated systemsby ensuring appropriate security controls and measures and taking internal defense actions. Includes access to system controls, monitoring, administration and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. SOURCE: National Initiative for Cybersecurity Careers and Studies

c. **IT Skills Community:** Skills needed to design, build, configure, operate and maintain IT, networks and capabilities. Includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate and dispose of IT as well as information resource management; and the management, storage, transmission and display of data and information. SOURCE: National Initiative for Cybersecurity Careers and Studies

d. **Cross-Functional Skills Community**: Skills required to lead, acquire and manage cyber initiatives; develop cyber workforce talent; and conduct cyberrelated legal and law enforcement activities. SOURCE: National Initiative for Cybersecurity Careers and Studies

e. **Work Role:** Detailed groupings of cyber and related work which include a list of attributes required to perform that role in the form of knowledge, skills and abilities (KSAs) and tasks performed in that role. SOURCE: NIST SP 800-181 Rev. 1