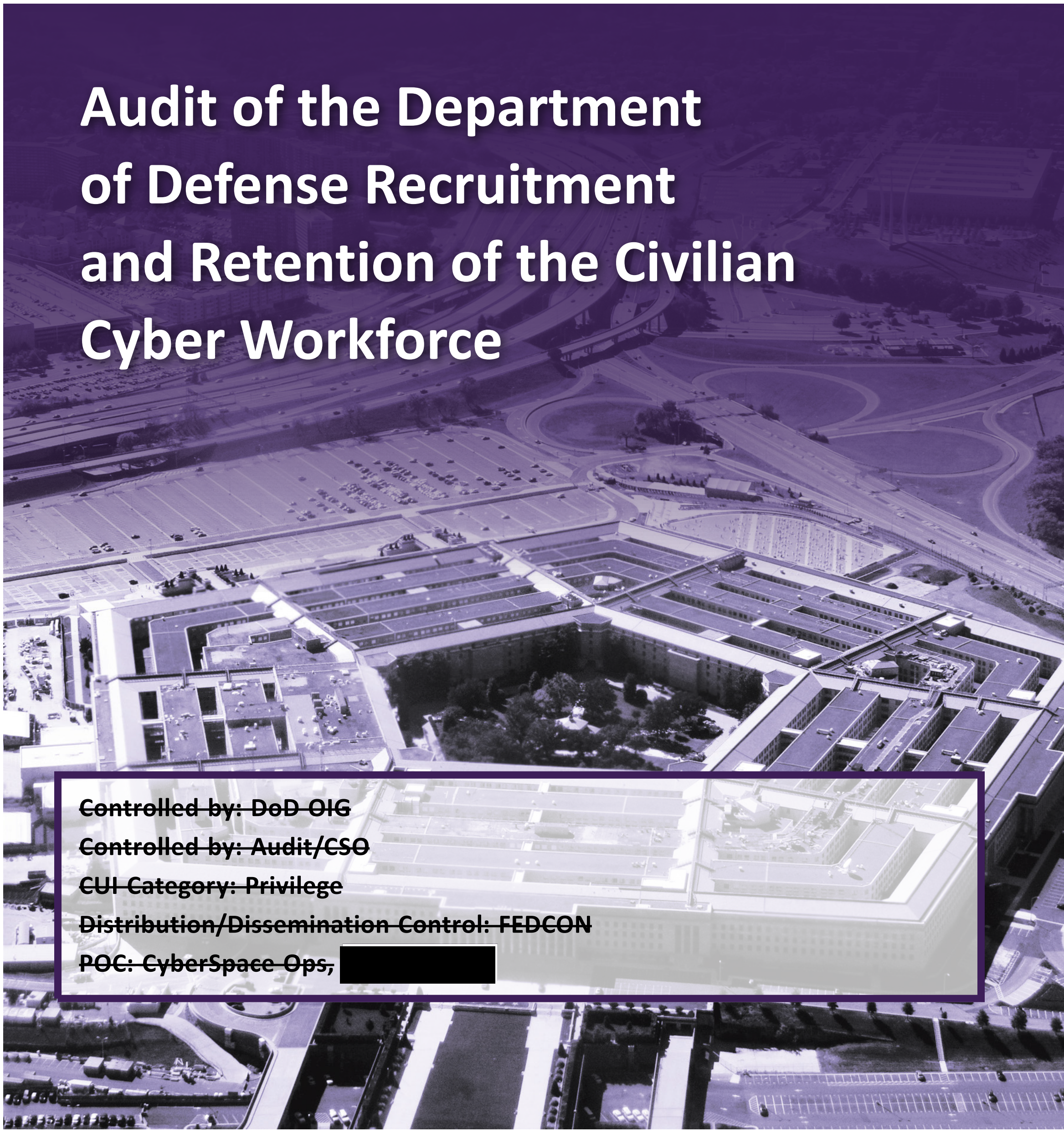
Report No. DODIG-2021-110

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 29, 2021



Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/CSO~~
~~CUI Category: Privilege~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: CyberSpace Ops,~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Results in Brief

Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce

July 29, 2021

Objective

The objective of this audit was to determine the extent to which the DoD is meeting Federal requirements, DoD guidance, and DoD strategic goals related to recruitment and retention programs for its civilian cyber workforce.

Background

In 2015, the Federal Cybersecurity Workforce Assessment Act required the coding of encumbered (filled) and vacant (unfilled) cyber positions across the Government based on the National Institute for Standards and Technology's cyber work role coding structure. According to the DoD civilian work role coding guidance (referred to in this report as the "DoD Coding Guide"), cyber work roles describe a set of responsibilities required to execute a function and consists of a definition as well as a representative list of tasks, knowledge, skills, and abilities. The DoD Coding Guide states that the selection of a cyber work role may provide enough information to ensure the identification and maintenance of the right skill set. In 2013, before the enactment of the Federal Cybersecurity Workforce Assessment Act, the DoD issued the DoD Cyberspace Workforce Strategy, which identifies multiple focus areas with critical elements for building and maintaining a competent and resilient cyber workforce. The 2013 strategy formed the foundation of follow-on DoD cyber strategies issued in 2015 and 2018. To assist in the recruitment and retention of the cyber workforce, the Office of the DoD Chief Information Officer (CIO) further implemented programs such as the DoD Cyber Scholarship Program, the DoD Cyber Information Technology Exchange Program, and initiated the Cyber Excepted Service (CES) personnel system.

Background (cont'd)

Findings

The Office of the DoD CIO took action to comply with the Federal Cybersecurity Workforce Assessment Act requirements by implementing the DoD Cyber Workforce Framework, issuing civilian work role coding guidance (DoD Coding Guide) to DoD Components, and submitting work roles of critical need to the Office of Personnel Management. However, the DoD Components did not code all positions in accordance with the DoD Coding Guide. Specifically:

- ~~(CUI)~~ [redacted] of the [redacted] core filled positions and [redacted] of the [redacted] non-core filled positions were not coded in accordance with the DoD Coding Guide; and
- ~~(CUI)~~ [redacted] of the [redacted] core unfilled positions and [redacted] of the [redacted] non-core unfilled positions were not coded in accordance with the DoD Coding Guide.

With the exception of the Department of the Army, the DoD Components we reviewed did not always comply with work role coding requirements because the DoD Components did not have a quality assurance process that ensured compliance with the DoD Coding Guide. The DoD may be unable to properly target its recruitment and retention efforts without completely and accurately coding all of its civilian cyber positions. We also found that the DoD took action to meet strategic goals related to recruitment and retention programs for its civilian cyber workforce. The Office of the DoD CIO further implemented the DoD Cyber Scholarship Program and the DoD Cyber Information Technology Exchange Program, began developing an enterprise-level aptitude test, and initiated the CES personnel system. However, until the DoD Components' application of work role codes is complete and accurate, the DoD may not have the information needed to identify and target the recruitment and retention programs to meet its greatest cyber workforce needs.

Results in Brief

Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce

Recommendations

We recommend that the DoD CIO:

- require DoD Components to code filled and unfilled positions to meet Federal requirements and comply with the DoD Coding Guide;
- in coordination with the Under Secretary of Defense for Personnel and Readiness and the Office of the Chief Data Officer, conduct a feasibility study of including quality assurance checks in systems used for coding civilian cyber workforce positions to ensure that work role coding is in accordance with the DoD Coding Guide; and
- based on the results of the feasibility study, establish and implement a manual or automated (or combination of both) quality assurance process to determine compliance with the DoD Coding Guide.

Management Comments and Our Response

The Acting DoD CIO agreed with the recommendations stating that DoD Components will complete work role coding by the end of 2021. He also stated that the DoD is developing an automated dashboard to show the status of the DoD Component configured manpower and personnel systems and the corresponding coded populations of the filled and unfilled cyber workforce positions. We will close the recommendations once we verify that the agreed-upon actions are complete.

Please see the Recommendations Table on the next page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Department of Defense Chief Information Officer	None	A.1, A.2, A.3	None

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 29, 2021

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE

SUBJECT: Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce (Report No. DODIG-2021-110)

This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

This report contains three recommendations all that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain open until we verify that the agreed-upon actions are complete.

Please provide us within 90 days documentation showing that the agreed-upon actions have been completed or a status of the actions in progress. Send your response to either [redacted] if unclassified or [redacted] if classified SECRET.
We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted]

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

Introduction

Finding A. The DoD Established Civilian Cyber Work Role Codes in Compliance With Federal Requirements, but Assignment of the Codes Was Not Complete or Accurate

Finding B. The DoD Took Action to Meet Strategic Goals for the Recruitment and Retention Programs of its Civilian Cyber Workforce

Appendixes

Contents (cont'd)

Management Comments

Introduction

Objective

The objective of this audit was to determine the extent to which the DoD is meeting Federal requirements, DoD guidance, and DoD strategic goals related to recruitment and retention programs for its civilian cyber workforce. See Appendix A for the scope and methodology and prior coverage.

Background

~~(CUI)~~ The DoD cyber workforce comprises military, civilian, and contractor personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. The DoD civilian cyber workforce consists of personnel in at least 48 occupational series, 10 of which are designated as "core" cyber occupational series.[1] According to DoD coding guidance (referred to in this report as the "DoD Coding Guide"), core cyber occupational series are those series in which every position is considered part of the cyber workforce.[2] [redacted] (see Appendix B for a full list of the 10 core cyber occupational series.) The non-core cyber occupational series are those series that may include cyber positions; however, cyber is not applicable to the entire series.[3] For example, personnel in the occupational series 0511-Auditor who conduct information technology audits are considered part of the non-core civilian cyber workforce. The DoD Coding Guide states that cyber work roles describe a set of responsibilities required to execute a function and consist of a definition as well as a representative list of tasks, knowledge, skills, and abilities. The selection of a cyber work role may provide enough information to ensure the identification and maintenance of the right skill set. For example, an auditor who conducts information technology audits would receive the cyber work role, 805 "IT Program Auditor."

[1] According to the DoD Cyber Workforce Identification and Coding Guide, an occupational series is a code or designation, for civilians, that is applied to a position or person that describes the work performed.

[2] Office of the DoD Chief Information Officer, "DoD Cyber Workforce Identification and Coding Guide," Version 1.0, August 31, 2017.

[3] For the purposes of this report, non-core cyber occupational series means that the occupational series is any occupational series that is not identified as one of the core cyber occupational series in the DoD Coding Guide.

~~(CUI)~~ As of November 2020, the Defense Civilian Personnel Advisory Service (DCPAS) reported that [redacted] core cyber occupational series positions and [redacted] non-core positions were filled within the DoD.[4] Table 1 identifies the distribution of those filled positions by the Military Departments and the Fourth Estate Agencies.[5]

Table 1. Distribution of the Civilian Cyber Workforce by DoD Component

~~(CUI)~~ DoD Component	Core Occupational Series Filled Positions	Non-Core Occupational Series Filled Positions	Total Civilian Cyber Workforce Filled Positions
Army	[redacted]	[redacted]	[redacted]
Navy	[redacted]	[redacted]	[redacted]
Air Force	[redacted]	[redacted]	[redacted]
Fourth Estate Agencies	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted] ~~(CUI)~~

Source: The DCPAS.

Federal Cybersecurity Workforce Assessment Act

In December 2015, Congress passed the Consolidated Appropriations Act of 2016, which enacted the Federal Cybersecurity Workforce Assessment Act (FCWAA) of 2015.[6] According to the legislation introduced in Senate Bill S. 2007, August 6, 2015, 114th Congress (2015-2016), the FCWAA's purpose is to "create a consistent framework to expedite the recruitment of highly qualified personnel who perform information technology, cybersecurity, and cyber-related functions to enhance cyber security across the Federal Government." Under the FCWAA, the heads of all Federal agencies were required to identify all encumbered (filled) and vacant (unfilled) information technology, cybersecurity, or other cyber-related positions and assign an "employment code" to each position. The FCWAA required the Director of the Office of Personnel Management (OPM), through the National Institute of Standards and Technology, to establish unique numeric employment codes for each of the cyber work roles and specialty areas defined in the National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework.[7] No later than 9 months after the enactment of the FCWAA, OPM

[4] The DCPAS develops and oversees civilian human resource plans, policies, and programs for DoD employees.

[5] The Fourth Estate comprise organizational entities that are not part of the Military Departments or combatant commands.

[6] Public Law 114-113, "The Consolidated Appropriations Act 2016," Section 301 to Section 304, "Federal Cybersecurity Workforce Assessment," December 18, 2015.

[7] The National Institute of Standards and Technology established the NICE Cybersecurity Workforce Framework in 2011 to define the personnel that held industry-recognized cyber certifications and associated training.

was required to establish procedures to identify all Federal civilian positions requiring the performance of information technology, cybersecurity, or other cyber-related functions. Federal agencies were required to establish procedures to identify and assign the employment codes within 3 months after the National Institute of Standards and Technology issued the codes. The DoD Cyber Workforce Framework (DCWF) is the DoD's version of the NICE Cybersecurity Workforce Framework. The DoD established guidance on the application of DCWF work role codes in the DoD Coding Guide.

Once the Federal agencies established the procedures, they had 1 year to complete the coding. According to a memorandum from the Acting DoD Chief Information Officer (CIO), DoD Components were required to code all civilian cyber workforce positions by April 15, 2018.[8] The FCWAA also required that the Federal agencies, beginning no later than 1 year after the date that the employment codes were assigned and annually thereafter through 2022:

- identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agencies workforce; and
- submit a report to the OPM Director describing those roles and substantiating the critical need designation.[9]

According to an OPM memorandum, by April 2019, agencies were to report their greatest skill shortages; analyze the root cause of the shortages; and provide action plans, targets, and measures for mitigating the critical skill shortages.[10] Based on the agency reports, OPM was to identify the skill shortages from a Government-wide perspective.

DoD Cyber Workforce Strategies

In 2013, the DoD issued its first DoD Cyberspace Workforce Strategy (DCWS), which identifies 6 strategic focus areas and 27 critical elements for building and maintaining a competent and resilient cyber workforce. Since the DCWS was issued, the DoD has issued two additional strategies that include cyber workforce elements—the 2015 DoD Cyber Strategy and the 2018 DoD Cyber Strategy. We do not discuss the 2015 strategy because the 2018 strategy superseded it. We define strategic goals as specific elements identified in the 2013 DCWS and

[8] DoD CIO memorandum, "Identifying and Coding Department of Defense Civilian Cyber Workforce Positions," September 14, 2017.

[9] Due to the challenges facing agencies during the coronavirus disease-19 pandemic, OPM suspended the requirement for agencies to submit the 2020 report; however, OPM implemented an alternative strategy to meet the FCWAA requirement. In April 2021, the Office of the DoD CIO submitted the DoD's FY 2021 work roles of critical need to OPM.

[10] OPM memorandum, "Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need," April 2, 2018.

specific sub-objectives identified in the 2018 Cyber Strategy, Line of Effort 8 (LoE 8), "Sustain a Ready Cyber Workforce" related to recruitment and retention programs for the DoD civilian cyber workforce.

DoD Cyberspace Workforce Strategy

On December 4, 2013, the Acting Deputy Secretary of Defense signed the DCWS, which is the overarching enterprise guidance for reshaping the DoD cyber workforce and includes approaches to recruit, train, and retain the workforce in a competitive national environment. The DCWS contains one focus area specific to recruitment and one specific to retention of the cyber workforce. Those focus areas and corresponding critical elements are as follows.

- Recruiting - Employ a multi-dimensional approach to recruiting.
    - Develop awareness of the unique cyberspace workforce opportunities at the DoD.
    - Partner with the Federal sector to develop a national cyberspace talent pipeline.
    - Foster non-traditional hiring for niche mission needs.
    - Create transition opportunities between and within military and civilian service.
    - Assess aptitude as well as qualifications.
- Retention - Retain qualified personnel.
    - Provide career progression and meaningful challenges.
    - Offer training opportunities tied to commitments.
    - Retain qualified performers with compensation programs.
    - Identify and retain cyberspace leaders.

2018 DoD Cyber Strategy

~~(U//FOUO)~~ On September 18, 2018, the Secretary of Defense signed the 2018 DoD Cyber Strategy, which emphasizes the importance of developing the DoD cyber workforce by identifying, recruiting, and retaining cyber personnel; developing processes to maintain visibility of the workforce; providing professional development opportunities; and partnering with industry and academia to establish standards in training and education to facilitate the growth of the workforce. The strategy assigns "offices of primary responsibility" for its implementation and execution. [redacted]

~~(U//FOUO)~~ LoE 8, "Sustain a Ready Cyber Workforce," contains 9 objectives and 38 sub-objectives, and the Office of the DoD CIO and the Office of the Chairman of the Joint Chiefs of Staff serve as the offices of responsibility for LoE 8. One of the nine objectives and seven sub-objectives covers enhancing and improving the identification and lifecycle management of the civilian cyber workforce. The following bullets identify the seven sub-objectives for the objective.

- Mature the implementation of the Cyber Excepted Service (CES) personnel system across the DoD.
- Mature the policies for the identification and coding of civilian manpower requirements and cyber work roles; and personnel skillsets and qualifications.
- Execute the DoD Cyber Workforce Critical Needs Assessment Process.
- Explore and assess the need for a DoD Cyber talent management program.
- Improve civilian recruitment and retention through the development and implementation of enhanced programs for the cyber workforce.
- Integrate and align the DCWF into the CES and other DoD civilian occupational structures.
- In partnership with OPM, explore the establishment of a Federal cyber position classification standard and occupational series.

DoD Civilian Cyber Workforce Recruitment and Retention Programs

Since FY 2001, various National Defense Authorization Acts (NDAAs) have established and authorized programs for the recruitment and retention of the DoD civilian cyber workforce. Those programs include the DoD Cyber Scholarship Program (CySP), the DoD Cyber Information Technology Exchange Program (CITEP), and the CES personnel system.

DoD Cyber Scholarship Program

The FY 2001 NDAA, as amended by the FY 2018 NDAA, established the CySP (formerly the DoD Information Assurance Scholarship Program).[11] The purpose of the program is to recruit and retain personnel for cyber workforce development at select institutions of higher education. The Office of the DoD CIO is responsible for the program, policy, and guidance, and the National Security Agency oversees the administration and execution of the program. DoD Components identify requirements, provide billets, select scholars, provide internships, and

[11] Public Law 106-398, "The National Defense Authorization Act for Fiscal Year 2001," Section 2200, "Programs; purpose," October 30, 2000. Public Law 115-91, "The National Defense Authorization Act for Fiscal Year 2018," Section 1649, "Cyber Scholarship Program," December 12, 2017.

hire graduates. The scholarship requires a service commitment, the length of which depends on whether the scholarship is for recruitment or retention. For recruitment, the service commitment is 1 year for every year or partial year of scholarship. For retention, the service commitment is three times the length of the scholarship period.

DoD Cyber Information Technology Exchange Program

The FY 2010 NDAA, as amended by the FY 2014 and FY 2017 NDAAs, established the CITEP.[12] The CITEP authorizes the temporary detail of DoD and private sector employees who work in the field of cyber operations or information technology to participate in an exchange between the two sectors. The program provides an opportunity for DoD Components and private sector organizations to share best practices, gain a better understanding of cross-sector information technology operations and challenges, and partner to address these challenges. Additionally, the program is an opportunity for DoD civilians to enhance cyber competencies and technical skills. The Office of the DoD CIO serves as the DoD administrator for CITEP and provides implementing guidance to the DoD Components. The CITEP is open to DoD civilian employees, GS-11 and above (or equivalent), considered to be exceptional employees and expected to assume increased cyber operations or information technology responsibilities in the future. Participants are required to return to their employing Component upon completion of the detail for a time equal to the length of the detail.

DoD Cyber Excepted Service

The FY 2016 NDAA authorized the DoD to establish an enterprise-wide approach for managing civilian cyber professionals through the CES personnel system.[13] The CES applies to DoD positions in which the employees perform, manage, supervise, or support functions necessary to execute the responsibilities of the U.S. Cyber Command (USCYBERCOM) as the Secretary of Defense determines necessary.

DoD Instruction 1400.25, Volume 3001, states that the CES serves as the civilian excepted service personnel system for cyber positions as designated by the DoD CIO in consultation with the Under Secretary of Defense for Personnel and

[12] Public Law 111-84, "The National Defense Authorization Act for Fiscal Year 2010," Section 1110, "Pilot program for the temporary exchange of information technology personnel," October 28, 2009. Public Law 113-66, "The National Defense Authorization Act for Fiscal Year 2014," Section 1106, "Extension of program for exchange of information-technology personnel," December 26, 2013. Public Law 114-328, "The National Defense Authorization Act for Fiscal Year 2017," Section 1123, "Modification to information technology personnel exchange program," December 23, 2016.

[13] Public Law 114-92, "The National Defense Authorization Act for Fiscal Year 2016," Section 1599f, "United States Cyber Command Recruitment and Retention," November 25, 2015.

Readiness, the Under Secretary of Defense for Policy, and the DoD Component heads.[14] According to an official from the Office of the DoD CIO, the CES applies to positions at USCYBERCOM and at supporting Components, including the Office of the DoD CIO Cybersecurity directorates, Joint Force Headquarters-DoD Information Network (JFHQ-DODIN), Defense Information Systems Agency (DISA), the Office of the Principal Cyber Advisor, the Joint Artificial Intelligence Center, and the Service Cyber Components. On April 16, 2021, an official from the Office of the DoD CIO stated that approximately 9,000 positions are designated as CES positions.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[15] We identified internal control weaknesses in the DoD's implementation of the FCWAA and the DoD Coding Guide. We will provide a copy of the report to the senior official responsible for internal controls in the Office of the DoD CIO, Departments of the Army (DA), Navy (DON), and Air Force (DAF).

[14] DoD Instruction 1400.25, Volume 3001, "DoD Civilian Personnel Management System: Cyber Excepted Service Introduction," August 15, 2017.

[15] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding A

The DoD Established Civilian Cyber Work Role Codes in Compliance With Federal Requirements, but Assignment of the Codes Was Not Complete or Accurate

The Office of the DoD CIO took action to comply with the FCWAA requirements by implementing the DCWF, issuing civilian work role coding guidance to DoD Components, and submitting work roles of critical need to OPM.[16] However, the DoD Components had not coded or had incorrectly coded some of their civilian cyber workforce positions.[17]

- ~~(CUI)~~ Of the [redacted] filled cyber workforce positions we reviewed, [redacted] of the [redacted] core positions ([redacted] percent) and [redacted] of the [redacted] non-core positions ([redacted] percent) were not coded in compliance with the DoD Coding Guide.
- ~~(CUI)~~ Of the [redacted] unfilled cyber workforce positions we reviewed, [redacted] of the [redacted] core positions ([redacted] percent) and [redacted] of the [redacted] non-core positions ([redacted] percent) were not coded in compliance with the DoD Coding Guide.

The DCWF work role coding was incomplete or incorrect because (with the exception of the DA) the DoD Components we reviewed did not have a quality assurance process that ensured DCWF work role coding complied with the DoD Coding Guide. As a result, the DoD may be unable to accurately determine the skill set and size of its civilian cyber workforce. Without coding all positions (filled and unfilled), the DoD may develop incorrect workforce planning activities, such as recruitment and retention strategies, and incorrectly report on work roles of critical need.

The DoD's Compliance With the FCWAA

To meet FCWAA requirements, the Office of the DoD CIO implemented the DCWF, issued guidance for assigning the DCWF work role codes to the DoD civilian cyber workforce positions, and submitted its work roles of critical need to OPM.[18]

[16] The work roles of critical need are positions deemed by the agency as having the greatest skill shortage.

[17] For the purposes of this report, incorrectly coded means that the codes were not assigned in accordance with the DoD Coding Guide. We modified the application of one rule due to the lack of impact on recruitment and retention efforts. We did not validate the job duties of the workforce against the codes.

[18] Public Law 114-113, "The Consolidated Appropriations Act 2016," Section 301 to Section 304, "Federal Cybersecurity Workforce Assessment," December 18, 2015.

The DoD Implemented the DCWF

The DCWF is the DoD's version of the NICE Cybersecurity Workforce Framework. The DCWF has 7 categories of cyber functions (roles and responsibilities) with 33 specialty areas and 54 work roles associated with the categories. See Table 2 for the seven categories and the description of each category. See Appendix C for the associated specialty areas, work roles, and DCWF work role codes.

Table 2. DCWF Categories

Categories	Descriptions
Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate	Investigates cybersecurity events or crimes related to information technology systems, networks, and digital evidence.
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology system performance and security.
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology systems and/or networks.
Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development.

Source: NICE Framework and DCWF.

The DoD Issued Work Role Coding Guidance

In September 2017, the Office of the DoD CIO issued the DoD Coding Guide to provide additional information on the DCWF and instructions on how to identify and code the existing civilian cyber workforce. The DoD Coding Guide defines the rules for applying the DCWF work role codes to DoD core and non-core cyber workforce positions. The DoD Coding Guide states that a position can receive up to three different DCWF work role codes. The first DCWF work role code assigned is considered the primary DCWF work role code, and the second and third DCWF work role codes are considered additional DCWF work role codes. The DoD Coding Guide includes the following rules.

- Core positions must have a primary DCWF work role code assigned.
- Non-core positions should have at least one additional DCWF work role code assigned if the primary work role code is zero-filled.

- Core and non-core positions should not have duplicate DCWF work role codes in the primary or additional work role code fields.
- Core and non-core positions should not have non-DCWF work role codes in the primary or additional work role code fields.

The DoD Submitted Work Roles of Critical Need

In April 2019, the Office of the DoD CIO submitted the DoD's work roles of critical need to OPM. Work roles of critical need are positions deemed by the agency as having the greatest skill shortages, in terms of:

- staffing levels or proficiency/competency levels and current and emerging shortages; and
- mission criticality or importance (that is, critical to meeting the agency's most significant organizational missions, priorities, and challenges).

~~(CUI)~~ To determine the work roles of critical need, the DoD CIO established a working group that comprised representatives from the Office of the DoD CIO, the Military Services, key Fourth Estate Components, the Joint Staff, the Principal Cyber Advisor, and the DCPAS. The working group members identified a list of civilian cyber DCWF work roles most critical to meeting their respective mission objectives and strategic goals and analyzed the vacancy rates for those positions. The working group concluded that the DoD's most critical work role needs as of April 2019 were [redacted] (work role code [redacted]) and [redacted] (work role code [redacted]) and submitted that information to OPM along with an action plan to mitigate the shortages in those work roles.

OPM canceled the requirement to submit work roles of critical need in FY 2020 because of the coronavirus disease-19 pandemic; instead, the Office of the DoD CIO submitted an action plan that addressed recruitment/outreach, hiring, retention, and system updates. In April 2021, the Office of the DoD CIO submitted the DoD's FY 2021 work roles of critical need to OPM.

DoD Civilian Cyber Workforce Coding Was Not Complete or Accurate

Although the Office of the DoD CIO took action to comply with the FCWAA, the DoD Components had not coded or had incorrectly coded some of their civilian cyber workforce positions. To determine whether the coding was complete and accurate, we applied requirements from the DoD Coding Guide to data obtained from the DCPAS for the filled positions and from the personnel systems or manpower systems of the DA, DON, and DAF for the unfilled positions.[19] We limited our review to the Military Departments for the unfilled positions because that data resides in the individual Component personnel or manpower systems. Table 3 provides the DoD Coding Guide requirements and the methodology used to determine compliance.

Table 3. Methodology Used to Determine Compliance With DoD Coding Guide Requirements

DoD Coding Guide Requirement	Methodology
Core positions must have a primary DCWF work role code assigned.	We reviewed the DCPAS and the Military Department personnel/manpower systems for all positions that had one of the 10 core cyber occupational series. If the primary code field was blank or zero-filled, the coding was considered incorrect.
Non-core positions should have at least one additional DCWF work role code assigned if the primary work role code is zero-filled.	We reviewed the DCPAS and the Military Department personnel/manpower systems for all positions with an occupational series other than the 10 core cyber occupational series and zeroes in the primary code field. If the primary code was zero-filled and an additional code was not assigned, the coding was considered incorrect.
Core and non-core positions should not have duplicate DCWF work role codes in the primary or additional work role code fields.	We reviewed the DCPAS and the Military Department personnel/manpower systems for duplicate DCWF work role codes assigned to a specific position. If duplicate DCWF work codes were identified, the coding was considered incorrect.
Core and non-core positions should not have Non-DCWF codes in the primary or additional work role code fields.	We reviewed the DCPAS and the Military Department personnel/manpower systems for any DCWF work role codes in the primary or additional work role code fields that were not cyber work role codes as defined in the DCWF. If the code was not a DCWF work role code, the coding was considered incorrect.

Source: The DoD Coding Guide.

Filled Positions

~~(CUI)~~ Of the [redacted] filled cyber workforce positions we reviewed, [redacted] of the [redacted] core positions ([redacted] percent) and [redacted] of the [redacted] non-core positions ([redacted] percent) were not coded in compliance with the DoD Coding Guide. Specifically, [redacted] of the core positions did not have a DCWF work role code assigned or the primary work role code was zero-filled, [redacted] had duplicate codes assigned, and [redacted] had non-DCWF work role codes assigned. Table 4 provides

[19] We did not determine whether the work force codes were correct with respect to the employee's actual work responsibilities, but only whether the coding complied with the DoD Coding Guide. The DA and DAF data for unfilled positions came from DA and DAF personnel systems, while the DON data came from the DON's personnel system, as well as its manpower systems. We obtained the data from the DCPAS in November 2020; and the DA, and DON data in February 2021. We received data from the DAF in February 2021; however, the data did not meet the standards of our request. Therefore, we relied on a previous data set from July 2020 from the DAF for this analysis.

~~(CUI)~~ the number of incomplete and incorrect DCWF work role codes for the core filled cyber occupational series positions by the Military Departments and Fourth Estate Agencies.

Table 4. DoD Core Cyber DCWF Work Role Coding – Filled Positions

~~(CUI)~~ DoD Component*	Core Occupational Series Filled Positions Identified	Number of Positions Without Work Role Codes or Coded Incorrectly	Percentage of Positions Without Work Role Codes or Coded Incorrectly
Army	[redacted]	[redacted]	[redacted]
Navy	[redacted]	[redacted]	[redacted]
Air Force	[redacted]	[redacted]	[redacted]
Fourth Estate Agencies	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted] ~~(CUI)~~

* The DA and DAF computations include the National Guard.
Source: The DCPAS and the DoD OIG.

~~(CUI)~~ Of the [redacted] non-core positions not coded in compliance with the DoD Coding Guide, [redacted] did not have an additional DCWF work role code assigned, [redacted] had duplicate DCWF work role codes assigned, and [redacted] had non-DCWF work role codes assigned.

Unfilled Positions

~~(CUI)~~ Of the [redacted] unfilled cyber workforce positions we reviewed, [redacted] of the [redacted] core positions ([redacted] percent) and [redacted] of the [redacted] non-core positions ([redacted] percent) were not coded in compliance with the DoD Coding Guide. Specifically, of the [redacted] core positions not coded in compliance with the DoD Coding Guide, [redacted] did not have a DCWF work role code assigned or the primary DCWF work role code was zero-filled, [redacted] had duplicate DCWF work role codes assigned, and [redacted] had non-DCWF work role codes assigned.

~~(CUI)~~ Of the [redacted] non-core positions not coded in compliance with the DoD Coding Guide, [redacted] had non-DCWF work role codes assigned and [redacted] had duplicate DCWF work role codes assigned. The DON accounted for [redacted] of the positions, and the DAF accounted for [redacted] of the positions while the DA accounted for [redacted] of the positions.

DoD Components Need Quality Assurance Processes for DCWF Coding

With the exception of the DA, the DoD Components reviewed did not always comply with DCWF work role coding requirements because the DoD Components did not have a quality assurance process that ensured compliance with the DoD Coding Guide. Quality assurance is the systematic monitoring and evaluation of a project to ensure standards of quality either by manual or automated processes. The Army established an automated quality assurance process for the DCWF work role coding of its civilian cyber workforce positions. In September 2018, the Automated Nature of Action Cyber Workforce Coding Maintenance Tool Instructions were posted to the main page of the cyber coding tool within the Automated Nature of Action application. The instructions provided guidance on the DA's "cyber workforce project coding tool," which allows managers and supervisors to not only initially enter DCWF work role codes, but also to modify DCWF work role codes as applicable for all positions under their responsibility. The tool includes built-in quality assurance checks that assist managers and supervisors in coding positions in compliance with the DoD Coding Guide.

Although the DON issued guidance that included some quality assurance requirements it did not ensure compliance with the DoD Coding Guide. On January 31, 2019, the Assistant Secretary of the Navy (Manpower and Reserve Affairs) issued a memorandum, "Department of Navy Civilian Cyberspace Workforce Coding and Reconciliation," that included guidance on the maintenance and reconciliation of DCWF work role coding in the personnel systems for civilians performing cyber work. A DON official stated that commands have working groups to manage work role coding updates and reviews. The DAF did not establish a quality assurance process. However, according to a DAF official, the Air Force Personnel Center maintains a checklist that includes the selection of DCWF work role codes when a supervisor performs a personnel action. The DoD CIO should require DoD Components to code filled and unfilled positions to meet Federal requirements and comply with the DoD Coding Guide. The DoD CIO, in coordination with the Under Secretary of Defense for Personnel and Readiness and the Office of the Chief Data Officer, should conduct a feasibility study of including quality assurance checks in systems used for coding civilian cyber workforce positions to ensure that work role coding is in accordance with the DoD Coding Guide. Based on the results of the feasibility study, the DoD CIO should establish and implement a manual or automated (or combination of both) quality assurance process to determine compliance with the DoD Coding Guide.

The DoD May Not Properly Target Recruitment and Retention Efforts

~~(CUI)~~ The DoD may be unable to properly target its recruitment and retention efforts to specific skill sets without completely and accurately coding all of its civilian cyber positions (both filled and unfilled) as required by the FCWAA and in accordance with the DoD Coding Guide. With [redacted] percent of its filled and [redacted] percent of unfilled core positions not coded or coded incorrectly, the DoD may be unable to accurately determine the skill set and size of its civilian cyber workforce, which may hinder workforce planning activities, such as recruitment and retention strategies and determining the work roles of critical need.

Recommendations, Management Comments, and Our Response

Recommendation A.1

We recommend that the DoD Chief Information Officer require DoD Components to code filled and unfilled positions to meet Federal requirements and comply with the DoD Cyber Workforce Identification and Coding Guide.

DoD Chief Information Officer Comments

The Acting DoD CIO agreed, stating that in May 2020, the Office of the DoD CIO began requiring DoD Components to code filled and unfilled positions in accordance with Federal and DoD guidance. He also stated that as of June 2021, DoD Components entered, at a minimum, the primary work role in their manpower and personnel systems and would code the two remaining work roles by the end of 2021.

Our Response

Comments from the Acting DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Office of the DoD CIO asserts that all work roles for filled and unfilled positions are updated and we verify that the work role coding is complete.

Recommendation A.2

We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Personnel and Readiness and the Office of the Chief Data Officer, conduct a feasibility study of including quality assurance checks in systems used for coding civilian cyber workforce positions to ensure that work role coding is in accordance with the DoD Cyber Workforce Identification and Coding Guide.

DoD Chief Information Officer Comments

The Acting DoD CIO agreed, stating that the DoD CIO completed a study in 2019 and is in the process of developing a cyber workforce common data model using the Advana platform. The model includes billet and position data in a standardized format and allows for conducting analytics that measure recruitment and retention key performance indicators.

Our Response

Comments from the Acting DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Office of the DoD CIO provides documentation that shows the Advana platform includes quality assurance checks to ensure that work role coding is in accordance with the DoD Cyber Workforce Identification and Coding Guide and we verify the full development of the Advana platform.

Recommendation A.3

We recommend that the DoD Chief Information Officer, based on the results of the feasibility study, establish and implement a manual or automated (or combination of both) quality assurance process to determine compliance with the DoD Cyber Workforce Identification and Coding Guide.

DoD Chief Information Officer Comments

The Acting DoD CIO agreed, stating that the DoD CIO began developing and leveraging the Advana platform in August 2020 to gain visibility of military and civilian workforce coding and has been updating manpower and personnel systems to include DoD Cyber Workforce Framework work role codes. The Acting DoD CIO stated that once those actions are complete, the Office of the DoD CIO will create a dashboard view of appropriately configured systems and the corresponding coded populations of filled and unfilled positions and identify systems that were not compliant.

Our Response

Comments from the Acting DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Office of the DoD CIO provides documentation that shows the Advana platform includes quality assurance checks to ensure that work role coding is in accordance with the DoD Cyber Workforce Identification and Coding Guide and we verify the full development of the Advana platform.

Finding B

The DoD Took Action to Meet Strategic Goals for the Recruitment and Retention Programs of its Civilian Cyber Workforce

The DoD took action to meet strategic goals for the recruitment and retention programs of its civilian cyber workforce as identified in the DCWS and the 2018 Cyber Strategy, LoE 8, "Sustain a Ready Cyber Workforce." Specifically, the Office of the DoD CIO further implemented the CySP and the CITEP, and began developing an enterprise-level aptitude test. The Office of the DoD CIO also initiated the CES personnel system. Although we identified instances in which the programs were not being implemented DoD-wide, the Office of the DoD CIO continues to work with the Components to implement the programs. However, until the DoD Components completely and accurately assign DCWF work role codes required by the FCWAA (as discussed in Finding A), the DoD may not have the information needed to identify and target the recruitment and retention programs to meet its greatest cyber workforce needs.

The DoD Took Action to Meet Strategic Goals for Recruiting and Retaining its Civilian Cyber Workforce

The DoD took action to meet strategic goals identified in the DCWS and the 2018 Cyber Strategy, LoE 8, "Sustain a Ready Cyber Workforce." Specifically, the Office of the DoD CIO further implemented the CySP and the CITEP, and took action to develop an enterprise-level cyber-aptitude test. The Office of the DoD CIO also initiated the CES personnel system.

The DoD Cyber Scholarship Program

The Office of the DoD CIO's further implementation of the CySP meets the DCWS goal of linking scholarships to Federal opportunities and the 2018 Cyber Strategy goal to improve civilian retention through the development and implementation of enhanced programs for the cyber workforce. The FY 2001 NDAA, as amended by the FY 2018 NDAA, established the CySP (formerly the DoD Information Security Scholarship Program), which pays for undergraduate and graduate degrees in cyber security.[20]

[20] Public Law 106-398, "The National Defense Authorization Act for Fiscal Year 2001," Section 2200, "Programs; purpose," October 30, 2000. Public Law 115-91, "The National Defense Authorization Act for Fiscal Year 2018," Section 1649, "Cyber Scholarship Program," December 12, 2017.

When used for recruitment, the CySP offers applicants a scholarship for up to 2 years to complete their undergraduate degree. When used for retention, the CySP offers DoD employees scholarships to obtain a graduate degree. The CySP requires a service commitment, the length of which depends on whether the scholarship is for recruitment or retention. For recruitment, the service commitment is 1 year for every year or partial year of scholarship. For retention, the service commitment is three times the length of the scholarship period. The Office of the DoD CIO is responsible for the program, policy, and guidance, and the National Security Agency oversees the administration and execution of the program. Table 5 identifies the number of undergraduate applicants and scholarships awarded in 2017, 2018, and 2019.

Table 5. The Office of the DoD CIO's Use of the CySP for Recruitment

Fiscal Year	Applications Received	Scholarships Awarded
2019	410	132
2018	265	71
2017	209	40

Source: The DoD Cyber Scholarship Program, National Centers of Academic Excellence in Cybersecurity.

For retention, the Office of the DoD CIO did not offer the CySP in FY 2017 or FY 2018. A National Security Agency official stated that for FY 2017, the CySP received funding late in the fiscal year; therefore, there was not enough time to process applications before the start of the 2017 fall semester. The official also stated that for FY 2018, the National Defense University's College for Information and Cyberspace did not offer the Advanced Management Program, which was a large portion of the CySP. Without the National Defense University program, the only available programs were in-resident/full-time graduate programs at the Naval Postgraduate School and the Air Force Institute of Technology; therefore, instead of offering an incomplete program, CySP program officials decided not to offer the CySP in FY 2018. In FY 2019, CySP program officials received four retention scholarship applications and offered two scholarships.

The DoD Cyber Information Technology Exchange Program

The Office of the DoD CIO's further implementation of the CITEP meets the DCWS goal to offer rotational opportunities with industry and the 2018 Cyber Strategy goal to improve civilian retention through the development and implementation of enhanced programs for the cyber workforce. The FY 2010 NDAA, as amended by the FY 2014 and FY 2017 NDAAs, established the CITEP, which authorizes the temporary detail of DoD and private sector employees who work in the field of cyber operations or information technology to participate in an exchange between the two sectors.[21]

The CITEP provides an opportunity for DoD Components and private sector organizations to share best practices, gain a better understanding of cross-sector information technology operations and challenges, and partner to address these challenges. Additionally, the program is an opportunity for DoD civilians to enhance cyber competencies and technical skills. The CITEP is open to DoD civilian employees, GS-11 and above (or equivalent), considered to be exceptional employees and expected to assume increased cyber operations or information technology responsibilities in the future. Upon completion of the temporary detail, participants are required to return to their employing Component for a time equal to the length of the detail. The Office of the DoD CIO serves as the DoD administrator for the CITEP and provides implementing guidance to the DoD Components.

The FY 2010 NDAA allowed for a maximum of 10 CITEP allocations at any given time. The FY 2017 NDAA authorized the CITEP to expand to 50 allocations.[22] With the expansion of the CITEP allocations, the Office of the DoD CIO divested management of the program to the individual DoD Components. The DON has consistently approved the majority of the CITEP allocations and according to a DON official, the CITEP is a key enabler for the DON's acquisition workforce to stay current with the latest technology and that the Assistant Secretary of the Navy (Research, Development, and Acquisition) and the Secretary of the Navy are supportive of the program.

The DoD Cyber Aptitude Test

The DoD began developing an enterprise-level aptitude test to meet the DCWS goal to develop methods to assess aptitude for recruiting the cyber workforce. According to the DCWS, an aptitude test allows the DoD to increase the candidate pool for recruitment efforts by identifying current employees with a broad range of experience that can lead to a qualified cyber professional, in addition to using traditional knowledge-based qualifications for both military and civilian positions. In July 2019, the Office of the DoD CIO identified a list of aptitude tests that are

[21] Public Law 111-84, "The National Defense Authorization Act for Fiscal Year 2010," Section 1110, "Pilot program for the temporary exchange of information technology personnel," October 28, 2009. Public Law 113-66, "The National Defense Authorization Act for Fiscal Year 2014," Section 1106, "Extension of program for exchange of information-technology personnel," December 26, 2013. Public Law 114-328, "The National Defense Authorization Act for Fiscal Year 2017," Section 1123, "Modification to information technology personnel exchange program," December 23, 2016.

[22] The FY 2017 NDAA did not pass until December 23, 2016. The additional allocations were available for the Components to use in FY 2018.

used across the DoD. According to an official from the Office of the DoD CIO, after June 2019, the DoD received additional funding to support the development and validation of an enterprise-level aptitude test for a subset of the military population, but the official added that additional funding is required to address civilian personnel.

The Cyber Excepted Service

The Office of the DoD CIO's implementation of the CES meets the DCWS goal to explore the development of authorities to support the employment of a highly skilled cyber workforce and the 2018 Cyber Strategy goal to mature the implementation of the CES personnel system across the DoD. The FY 2016 NDAA authorizes the DoD to establish an enterprise-wide approach for managing civilian cyber professionals through the CES personnel system.[23] The CES is designed for civilian employees engaged in, or in support of, certain cyber-related missions.[24] Most civilian employees are hired through the competitive service; however, OPM provides excepted service hiring authorities to fill special positions or to fill positions in unusual or special circumstances. Table 6 provides a comparison between the competitive service and excepted service authorities.

Table 6. Competitive Service vs. Excepted Service

	Title 5 Competitive Service	Title 10 Excepted Service
Recruitment	Most unfilled positions are advertised on USA Jobs, and all eligible/qualified applicants must be considered.	No requirement to advertise on USA Jobs or elsewhere; applicant search (area of consideration) may be targeted to a geographic area or other criteria.
Compensation	Requires use of the General Schedule (GS) pay tables and limitations. All occupations are graded the same and receive the same level of compensation with few exceptions. Requires rigid adherence to pay setting regulations.	Enables market-sensitive pay structures but still subject to pay caps at the upper end of the scale. Enables flexible pay setting based on market value.
Career Advancement	Promotions generally require candidates to apply for a new position.	Enables candidates to advance based on their development and organizational need if qualification and budget factors are maintained.

[23] Public Law 114-92, "The National Defense Authorization Act for Fiscal Year 2016," Section 1599f, "United States Cyber Command Recruitment and Retention," November 25, 2015.

[24] Title 5, United States Code, "Government Organizations and Employees." Title 10, United States Code, "Armed Forces."

Table 6. Competitive Service vs. Excepted Service (cont'd)

	Title 5 Competitive Service	Title 10 Excepted Service
Promotion Process	Based on minimum time-in-grade. Requires 52 weeks at the next lower grade for promotion or placement to higher grade. Additionally, a higher graded billet must be available, a new higher graded billet established, or the current position description rewritten and reclassified at a higher level.	No time-in-grade requirements. Promotion or placement is based on the Component's assessment of the individual's qualifications and readiness for advancement.

Source: The DCPAS FY 2017-2022 Cyber Strategic Workforce Plan Report, January 2017.

The Office of the DoD CIO began a two-phased implementation of the CES in July 2016, with a planned completion in FY 2021. Phase 1 was completed in March 2018 and focused CES implementation at USCYBERCOM, JFHQ-DODIN, the Office of the DoD CIO Cybersecurity, the Office of the Principal Cyber Advisor, and the Joint Artificial Intelligence Center. Phase 2 is ongoing and focused on CES implementation at DISA and the Service Cyber Components. According to an official from the Office of the DoD CIO, as of May 2021, the Navy, Marine Corps, and Air Force Cyber Components and DISA had completed CES implementation and the Army Cyber Component is continuing their implementation efforts. The Office of the DoD CIO's goal is to have all Components complete implementation by the end of FY 2021, with the exception of the Army Cyber Component. The Army requested additional time because it relocated Army Cyber Command Headquarters from Fort Meade, Maryland, to Fort Gordon, Georgia, between June and September 2020.

In March 2019, the USCYBERCOM Commander testified before the House Armed Services Committee that the average time to hire cyber workforce professionals before the CES was 111 days; however, with the implementation of the CES, the average time to hire was reduced to approximately 44 days. According to an official from the Office of the DoD CIO, the CES applies to positions at USCYBERCOM and supporting Components, including the Office of DoD CIO Cybersecurity, JFHQ-DODIN, DISA, the Office of the Principal Cyber Advisor, the Joint Artificial Intelligence Center, and the Service Cyber Components. The official from the Office of the DoD CIO indicated that as of April 2021, approximately 9,000 positions were designated as CES positions and about 6,500 personnel were converted or hired into the CES.

The CES includes nine enhancements to further the recruitment and retention of a qualified civilian cyber workforce. As of June 2020, the Office of the DoD CIO has implemented two of the enhancements as shown in Table 7.

Table 7. Milestones for the Implementation of CES Enhancements

Enhancement	Description	Enhancement Status
Pathways and Scholarship Program	CES Policy (Volume 3005) allows graduates non-competitive conversion into the excepted service (CES).	Completed.
Program Evaluation	Provides an opportunity to understand the progress of CES, the link between the DoD's cyber needs and critical business outcomes, and direction for a longer term cyber hiring and retention strategy.	Completed.
Interchange Agreement	The DCPAS/DoD CIO have agreed to seek an indefinite Government-wide CES/Title 5 Interchange Agreement with OPM.	Staffed for signature; then will send to OPM.
Delegate Pay-Setting Authority at Steps 11/12 to CES Organizations	The DCPAS/DoD CIO have agreed to provide a process for delegating step 11 and 12 salary decisions to the Component level.	Completion target is for FY 2021 completion.
Targeted Local Market Supplement	Establishes as additions to the standard CES pay band and grade rate ranges, in response to labor market conditions.	Completion target is for January 2021.
Expansion of Retention Incentives	The DCPAS/DoD CIO will explore feasibility of expanding retention bonuses to cover selected CES work roles who are departing for other Federal service jobs.	Completion target is for end of FY 2021.
Ensure Component Supplemental Guidance is Complementary to Operationalizing CES	Current CES policy instructs DoD Component heads to comply with the philosophy and policy of the Secretary of Defense to keep supplementation of the CES volumes to a minimum and to eliminate regulations that are redundant or unnecessary.	Effort is ongoing.
Pay Banding	Current CES policy allows DoD Components seek to transition to a non-graded banded structure.	Completion target is FY 2024.
Rank In Person	Current CES policy allows DoD Components seek to transition to a rank-in-person construct.	Completion target is FY 2024.

Source: The Office of the DoD CIO.

According to an official from the Office of the DoD CIO, when the CES originally launched in 2016, the office focused on implementing the overall personnel system to allow the Components to hire faster. However, in FY 2019, the Office of the DoD CIO began developing policy for implementing the CES enhancements.

The DoD is Working to Implement Strategic Goals Widely, but Success Cannot Be Accurately Measured Until Positions Are Coded

As discussed in Finding A, the DoD Components' application of DCWF work role codes was not complete or accurate, which may prevent the DoD from properly targeting recruitment and retention efforts to specific skill sets. Until the Components' application of DCWF work role codes is complete and accurate, the DoD may not have the information available to identify and target recruitment and retention programs to meet its greatest cyber workforce needs.

Appendix A

Scope and Methodology

We conducted this performance audit from November 2019, through May 2021, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The scope of this audit was the implementation of Federal civilian cyber workforce requirements, DoD guidance, and DoD strategies focusing on the recruitment and retention of the civilian cyber workforce. We reviewed specific requirements in the 2015 FCWAA and specific guidance provided by the Office of the DoD CIO in the 2017 DoD Coding Guide. In addition to the specific requirements, we also reviewed specific elements of the 2013 DCWS and specific sub-objectives of LoE 8 from the 2018 DoD Cyber Strategy, as they related to recruitment and retention programs. We also reviewed the DoD's use of special hiring authorities, such as the CES to recruit and retain its civilian cyber workforce.

To determine the extent to which the DoD was meeting Federal civilian cyber workforce requirements and DoD guidance, we interviewed personnel from the Office of the DoD CIO, the DCPAS, DA, DON, and DAF; reviewed documentation; conducted site visits; and reviewed prior reports to determine whether the DoD implemented specific requirements of the FCWAA and DoD guidance. For the purposes of this report, incorrectly coded means that the codes were not assigned in accordance with the DoD Coding Guide. We did not assess the accuracy of the DCWF work role coding for filled or unfilled civilian cyber workforce positions. We also reviewed whether the DoD submitted the work roles of critical need to OPM.

We analyzed Defense Civilian Personnel Data System data as of November 2020 provided by the DCPAS for filled civilian workforce positions. The data provided by the DCPAS contained DA, DON, DAF, Fourth Estate Agencies, and Title 32 positions. Title 32 positions include the Army National Guard and Air National Guard. The DON data included Marine Corps positions; the Military Department data included Reserve and combatant command positions; and the Fourth Estate Agency data included organizational entities that are not part of the Military Departments or combatant commands. We reviewed 100 percent of the core filled and identified non-core cyber occupational series positions. To determine whether the positions were coded correctly, we applied four coding rules identified in the DoD Coding Guide.

The following four coding rules were tested.

- Core positions must have a primary DCWF work role code assigned. In addition, core positions with zero-filled fields were considered incorrect.
- Non-core positions should have at least one additional DCWF work role code assigned if the primary work role code is zero-filled.
- Core and non-core positions should not have duplicate DCWF work role codes in the primary or additional work role code fields. We excluded positions coded with duplicative zero-filled fields from the results in Finding A because of the lack of impact on recruitment and retention efforts.
- Core and non-core positions should not have non-DCWF codes in the primary or additional work role code fields.

We also analyzed Defense Civilian Personnel Data System data as of February 2021 provided by the DA and DON for unfilled civilian workforce positions. We received data for unfilled positions from the DAF in February 2021; however, the data did not meet the standards of our request. Therefore, we relied on a previous data set from July 2020 from the DAF for unfilled civilian workforce positions. DA and DAF data did not include the Title 32 positions. The DON data included Marine Corps positions, and the Military Department data included Reserve and combatant command positions. In addition, we analyzed the DON's manpower data as of February 2021. We reviewed 100 percent of the core unfilled and identified non-core cyber occupational series positions. We applied the same four coding rules as for the filled positions to the unfilled positions.

Office of the DoD CIO and DCPAS officials stated that the manpower system is the authoritative source for unfilled positions. A DA official stated that because unfilled positions were identified in the DA's personnel system, the data may not include all unfilled positions. We did not request DA manpower data because the DA official stated that the DA's manpower system does not have DCWF work role codes. According to a DAF official, the DAF was able to provide all unfilled positions because manpower interface data are linked to personnel position data; however we did not validate this. We determined that the DAF manpower system does not have DCWF work role codes. In addition to personnel system data, we also analyzed data from the DON's manpower systems, including DCWF work role codes. According to a DON official, identifying unfilled positions requires a manual comparison of the total number of manpower Billet Identification Numbers to the total number of personnel Billet Identification Numbers. We followed the DON guidance to identify unfilled positions. As a completeness and integrity check, we also reverse compared the DON personnel Billet Identification Numbers to the DON's manpower data to determine whether the manpower data were complete and identified discrepancies. While this discrepancy is a data integrity issue, we determined that the data were sufficiently reliable for the purpose of determining to what extent the DoD was meeting Federal civilian cyber workforce requirements and DoD guidance.

~~(CUI)~~ To assess the completeness and accuracy of the Defense Civilian Personnel Data System data (June 2020) from the DCPAS, we followed the guidance provided by the GAO's Financial Audit Manual, section 450 (Figure 450.1). To obtain a confidence level of 95 percent, using Excel's random number selection function, we randomly sampled 45 positions from each Military Department (45 of [redacted] DA positions; 45 of [redacted] DON positions; 45 of [redacted] DAF positions). We then compared the Defense Civilian Personnel Data System data provided by the DCPAS to the Defense Civilian Personnel Data System data provided by the DA (July 2020), DON (July 2020), and DAF (July 2020) and found no deficiencies. Specifically, for each sample item, we verified the electronic data interchange personal identifier (EDIPI) field and whether there was a DCWF work role code in the primary work role code field.

To determine the extent to which the DoD was meeting DoD strategic goals, we interviewed personnel from the Office of the DoD CIO, the DA, DON, and DAF, and USCYBERCOM, DISA, and JFHQ-DODIN; reviewed documentation; and conducted site visits to determine whether the DoD implemented DoD strategic goals. The goals were specific to recruitment and retention of the civilian cyber workforce.

We reviewed whether the DoD made progress in implementing specific elements of the 2013 DCWS and specific sub-objectives of the 2018 DoD Cyber Strategy, "LoE 8, Sustain a Ready Cyber Workforce," as they related to elements within the 2013 DCWS. We reviewed the progress made in the implementation of critical elements for two of the six focus areas in the 2013 DCWS.

For focus area two of the 2013 DCWS, which was to employ a multi-dimensional approach to recruiting, we reviewed the following critical elements.

- Assess aptitude as well as qualifications.
- Create transition opportunities between and within military and civilian service.
- Develop awareness of the unique cyberspace workforce opportunities at the DoD.
- Foster non-traditional hiring for niche mission needs.

For focus area four of the 2013 DCWS, which was to retain qualified personnel, we reviewed the following critical elements.

- Provide career progression and meaningful challenges.
- Offer training opportunities tied to retention commitments.
- Retain qualified performers via compensation programs.
- Identify and retain cyberspace leaders.

For the 2018 Strategy LoE 8 items, we reviewed specific sub-objectives that related to the 2013 DCWS. Those sub-objectives include:

- improve civilian recruitment and retention through the development and implementation of enhanced programs for the cyber workforce; and
- mature the implementation of the CES personnel system across the DoD.

We obtained information from the following Components.

- Office of the DoD CIO
- USCYBERCOM
- JFHQ-DODIN
- Office of the DoD CIO Cybersecurity
- DISA Headquarters
- Defense Civilian Personnel Advisory Service
- Headquarters, Department of Navy
- Assistant Secretary of the Navy (Manpower and Reserve Affairs) Task Force Innovation
- DON Office of Civilian Human Resources
- 10th Fleet/Navy Fleet Cyber Command
- Headquarters Marine Corps
- Marine Forces Cyber Command
- Headquarters Department of the Army
- Army Civilian Human Resources Agency
- Army Cyber Command
- Air Force Personnel Center
- 16th Air Force/Air Force Cyber Command
- National Security Agency

Use of Computer-Processed Data

We used computer-processed data extracted from Defense Civilian Personnel Data System and Military Department manpower systems to reach some conclusions in this report. We obtained Defense Civilian Personnel Data System data from the DCPAS, DA, DON, and DAF; and manpower data from the DON and DAF in order to determine whether filled and unfilled core and identified non-core occupational series positions were coded in accordance with Federal requirements and DoD guidance. We did not request DA manpower data because according to a DA official, DCWF work role codes are not in the manpower system.

~~(CUI)~~ To assess the completeness and accuracy of the Defense Civilian Personnel Data System data provided by the DCPAS, we followed the guidance provided by GAO's Financial Audit Manual, section 450 (Figure 450.1). To obtain a confidence level of 95 percent, using Microsoft Excel's random number selection function, we randomly sampled 45 positions from each Military Department (45 of [redacted] DA positions; 45 of [redacted] DON positions; 45 of [redacted] DAF positions). We then compared the Defense Civilian Personnel Data System data provided by the DCPAS to the Defense Civilian Personnel Data System data provided by the DA, DON, and DAF and found no deficiencies.[25] Specifically, for each sample item, we verified the EDIPI field and whether there was a DCWF work role code in the primary work role code field. In addition, we assessed the completeness and integrity of the DA, DON, and DAF Defense Civilian Personnel Data System data. We reviewed the entire dataset provided by the DA, DON, and DAF for duplication errors and missing elements. Specifically, for each data entry, we checked to see whether there were duplicate EDIPI numbers in the EDIPI field and whether each data entry had an EDIPI number. When we identified data discrepancies, we corroborated with the DCPAS and Military Department points of contact to determine the cause and to resolve the discrepancies. We found no exceptions and determined that the Defense Civilian Personnel Data System data from the DCPAS, DA, DON, and DAF were sufficiently reliable.

We found that the DON manpower data contained the DCWF work role codes and we reviewed the data for completeness and integrity by reviewing the entire dataset provided by the DON for duplication errors and missing elements. Specifically, for each data entry, we checked to see whether there were duplicate EDIPI numbers in the EDIPI field and whether each data entry had an EDIPI number. We also compared the DON personnel data to the DON manpower data to determine whether all the Billet Identification Numbers in the personnel system

[25] We did not test the reliability of National Guard data because the National Guard data comprises only 8 percent of the data within our review.

data were included in the manpower system data and identified discrepancies. We brought this issue to the attention of the DON point of contact. While this discrepancy is a data integrity issue, we determined that the data were sufficiently reliable for the purpose of determining to what extent the DoD was meeting Federal civilian cyber workforce requirements and DoD guidance. We did not assess the DAF data because we determined that the DAF did not add the DCWF work role codes to its manpower system.

We also obtained data from the Office of the DoD CIO and the National Centers of Academic Excellence in Cybersecurity to determine the frequency with which the different programs were used over several fiscal years. To assess the data from the Office of the DoD CIO and the National Centers of Academic Excellence in Cybersecurity, we corroborated the data with the DoD Components. For the purpose of determining the frequency with which the different programs were used over several fiscal years, the data were sufficiently reliable.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the DAF issued six reports discussing cyber workforce hiring authorities, talent management strategies, skill gap assessment needs, critical staffing needs, coding procedures, and identifying and maintaining a trained cyber workforce. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted Air Force Audit Agency reports can be accessed at https://www.afaa.af.mil/.

GAO

Report No. GAO-19-181, "Federal Workforce: Key Talent Management Strategies for Agencies to Better Meet Their Missions," March 28, 2019

> The GAO found that Federal work is changing amid demographic and technological trends. The GAO identified the following key trends affecting Federal work: (1) technological advances; (2) an increased reliance on non-Federal partners (for example, contractors or grantees); (3) fiscal constraints; (4) evolving mission requirements; and (5) changing demographics and shifting attitudes toward work. The GAO report stated that, given these trends, key talent management strategies can help agencies better manage the current and future workforce. These strategies include aligning human capital strategy with current and future mission requirements, acquiring and assigning talent, incentivizing and compensating employees, and engaging employees.

Report No. GAO-19-144, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," March 12, 2019

The GAO found that the 24 reviewed Federal agencies generally assigned work roles to filled and vacant positions that performed information technology, cybersecurity, or cyber-related functions as required by the FCWAA. However, 6 of the 24 agencies reported that they had not completed assigning the associated work role codes to their vacant positions, although they were required to do so by April 2018. In addition, most agencies likely miscategorized the work roles of many positions. Specifically, 22 of the 24 agencies assigned a "non-IT" work role code to 15,779 (about 19 percent) of their information technology positions within the 2210 occupational series. Furthermore, the six agencies that the GAO selected for additional review had assigned work role codes that were not consistent with the work roles and duties described in corresponding position descriptions for 63 of 120 positions within the 2210 occupational series that the GAO examined. The GAO found that the 24 agencies have begun to identify critical needs and submitted a preliminary report to OPM.

Report No. GAO-18-466, "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions," June 14, 2018

The GAO identified that 21 of the 24 agencies covered by the Chief Financial Officer's Act had submitted a report to Congress that included a baseline assessment of agency personnel with professional certifications. However, the GAO concluded that results of the agency assessments may not have been reliable because the agencies did not address all of the reportable information and were limited in their ability to obtain complete and consistent information about the certifications held by agency personnel.

Report No. GAO-16-686, "Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority Recommendation Status," August 26, 2016

The GAO identified that the Chief Information Security Officers at 24 agencies identified key challenges they faced in fulfilling their responsibilities, including the sufficiency of their cybersecurity workforce to implement the number and scope of security requirements and the ability to offer salaries that were competitive with the private sector for candidates with high-demand technical skills. Furthermore, the Chief Information Security Officers stated that certain security personnel lacked the skill sets needed or were not sufficiently trained.

Report No. GAO-16-521, "Federal Hiring: Office of Personnel Management Needs to Improve Management and Oversight of Hiring Authorities," August 2, 2016

> The GAO found that of the 105 hiring authorities used in FY 2014, agencies relied on 20 for 91 percent of the 196,226 new appointments made that year. The competitive examining hiring authority, generally seen as the traditional method for Federal hiring, was the single most used authority in FY 2014, but accounted for less than 25 percent of all new appointments. While OPM tracks data on agency time-to-hire, manager and applicant survey results, and compliance audits to assess the hiring process, this information is not used by OPM or agencies to analyze the effectiveness of hiring authorities. As a result, OPM and agencies do not know whether authorities are meeting their intended purposes.

Air Force

Report No. F2020-0002-O10000, "Cybersecurity Workforce Improvement Program," October 25, 2019

> Air Force personnel did not identify all cybersecurity personnel or comply with cybersecurity workforce qualification requirements. Specifically, personnel did not properly identify 21 percent of cybersecurity personnel or complete one or more qualification requirements for all cybersecurity personnel reviewed. Identifying all cybersecurity personnel is essential to DoD current and long-term initiatives to manage critical cybersecurity personnel resources.

Appendix B

DoD Cyber Workforce Coding Guidance

The "DoD Cyber Workforce Identification and Coding Guide, Version 1.0," August 31, 2017, provides a listing of potential occupational series related to cyber. The occupational series fall into four categories (core cyber, tier 1—strong cyber relationship, tier 2—some cyber roles, and common occupations—may have cyber roles). The guide states that a core cyber occupation means that every position within the occupation is cyber. Table 8 identifies the core cyber occupational series.

Table 8. The DoD's Core Cyber Occupational Series

~~(CUI)~~ Occupational Series	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted] ~~(CUI)~~

Source: The DoD Cyber Workforce Identification and DoD Coding Guide, as modified on September 25, 2017.

Appendix C

DoD Cyber Workforce Framework

The "DoD Cyber Workforce Framework, Version 3.1," establishes a standard lexicon for cyber work roles. Table 9 identifies the 7 categories of cyber functions, with 33 specialty areas and 54 work roles associated with the categories.

Table 9. DoD Cyber Workforce Framework

~~(CUI)~~ Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
Analyze	Threat Analysis	Warning Analyst	141	Collects, processes, analyzes, and disseminates cyber warning assessments.
	Exploitation Analysis	Exploitation Analyst	121	Identifies access and collection gaps, leverages resources and techniques to penetrate targeted networks.
	All-Source Analysis	All-Source Analyst	111	Analyzes data and submit intelligence requirements to support plans and operations.
		Mission Assessment Specialist	112	Develops assessment plans and measures of performance/ effectiveness.
	Targets	Target Developer	131	Performs target analysis from intelligence, coordinates partner activities, and presents targets for vetting.
		Target Network Analyst	132	Conducts collection and source data analysis to ensure target continuity and operation.
		[redacted]	[redacted]	[redacted]
	Language Analysis	Multi-Disciplined Language Analysis	151	Applies language and cultural expertise with target/threat information to disseminate intelligence data. ~~(CUI)~~

Table 9. DoD Cyber Workforce Framework (cont'd)

~~(CUI)~~ Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
Collect and Operate	Collection Operations	All-Source Collection Manager	311	Identifies collection authorities and capabilities of collection assets and monitors collection actions.
		All-Source Collections Requirements Manager	312	Evaluates and monitors performance of collection assets and operations and develops strategies.
	Cyber Operational Planning	Cyber Intelligence Planner	331	Develops intelligence plans to satisfy cyber operation needs. Participates in validation of cyber actions.
		Cyber Operations Planner	332	Develops support plans for cyber operations and participates in targeting selection of cyber actions.
		Partner Integration Planner	333	Advances cooperation between cyber partners. Provides best practices and support for cyber actions.
	[redacted]	[redacted]	[redacted]	[redacted]
		[redacted]	[redacted]	[redacted]
Investigate	Cyber Investigation	Cyber Crime Investigator	221	Identifies, examines, and preserves evidence using documented analytical and investigative techniques.
	Digital Forensics	Forensics Analyst	211	Investigates computer-based crimes establishing evidence associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	212	Analyzes digital evidence and investigates computer security incidents to support vulnerability mitigation. ~~(CUI)~~

Table 9. DoD Cyber Workforce Framework (cont'd)

~~(CUI)~~ Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
Operate and Maintain	Data Administration	Database Administrator	421	Administers databases and data management systems allowing for storage, query, and utilization of data.
		Data Analyst	422	Designs and implements algorithms and processes for data used for modeling, data mining, and research.
	Knowledge Management	Knowledge Manager	431	Manages processes to identify, document, and access intellectual capital and information.
	Customer Service and Technical Support	Technical Support Specialist	411	Provides technical support to customers in accordance with established processes.
	Network Services	Network Operations Specialist	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration	System Administrator	451	Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts.
	Systems Analysis	Systems Security Analyst	461	Analyzes and develops the integration, testing, operations, and maintenance of systems security.
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor	731	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Compliance Manager	732	Develops and oversees privacy program, supports privacy compliance needs of executives and their teams. ~~(CUI)~~

Table 9. DoD Cyber Workforce Framework (cont'd)

~~(CUI)~~

Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer	711	Develops, plans, coordinates, and evaluates cyber training/ education courses, methods, and techniques.
		Cyber Instructor	712	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management	Information Systems Security Manager	722	Responsible for the cybersecurity of a program, organization, system, or enclave.
		COMSEC Manager	723	Manages the Communications Security (COMSEC) resources of an organization.
	Strategic Planning and Policy	Cyber Workforce Developer and Manager	751	Develops cyberspace workforce plans, strategies, and guidance to support personnel and training.
		Cyber Policy and Strategy Planner	752	Develops plans, strategy, and policy to support and align with organizational cyber missions and initiatives.
	Executive Cyber Leadership	Executive Cyber Leadership	901	Executes authorities and establishes direction for an organization's cyber-related resources and operations.
	Acquisition and Program/Project Management	Program Manager	801	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program.
		IT Project Manager	802	Manages information technology projects to provide a unique service or product.
		Product Support Manager	803	Manages functions needed to field and maintain readiness and capabilities of systems and components. ~~(CUI)~~

Table 9. DoD Cyber Workforce Framework (cont'd)

~~(CUI)~~ Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
		IT Investment/ Portfolio Manager	804	Manages information technology capabilities that align with mission and business enterprise priorities.
		IT Program Auditor	805	Evaluates information technology programs to determine compliance with standards.
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst	511	Collects data from cyber defense tools to analyze events for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist	521	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response	Cyber Defense Incident Responder	531	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst	541	Assesses systems and networks and identifies deviations from acceptable configurations or policy.
Securely Provision	Risk Management	Authorizing Official/Designating Representative	611	Assumes responsibility for information systems operating at an acceptable level of risk.
		Security Control Assessor	612	Assesses effectiveness of security controls employed with or inherited by information technology systems.
	Software Development	Software Developer	621	Develops, creates, maintains, and codes computer applications, software, or specialized utility programs.
		Secure Software Assessor	622	Analyzes security of applications, software, or specialized utility programs and provides actionable results. ~~(CUI)~~

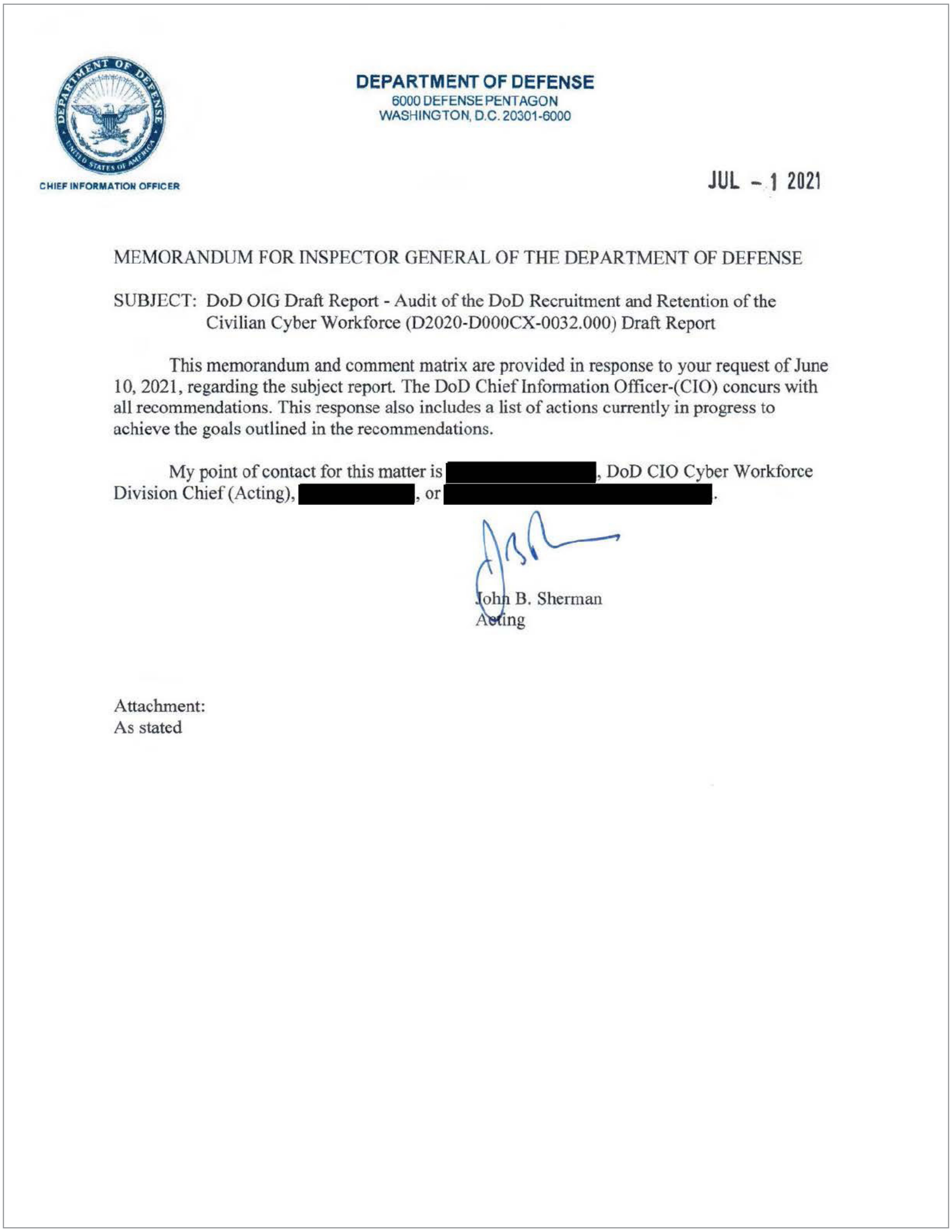
Table 9. DoD Cyber Workforce Framework (cont'd)

~~(CUI)~~ Category	Specialty Area	Work Role	DCWF Code	Work Role Definition
	Systems Architecture	Enterprise Architect	651	Develops and maintains information systems and processes to support enterprise mission needs.
		Security Architect	652	Designs enterprise and systems security throughout the systems development lifecycle.
	Technology R&D	Research & Development Specialist	661	Conducts systems engineering and research to develop new capabilities, fully integrating cybersecurity.
	Systems Requirements Planning	Systems Requirements Planner	641	Consults with customers to evaluate functional requirements and translate into technical solutions.
	Test and Evaluation	System Testing and Evaluation Specialist	671	Plans, prepares, executes, and analyzes systems tests to evaluate results against requirements.
	Systems Development	Information Systems Security Developer	631	Designs, develops, and tests information system security throughout the systems development lifecycle.
		Systems Developer	632	Designs, develops, and tests information systems throughout the systems development lifecycle. ~~(CUI)~~

Source: DCWF Work Role Tool.

Management Comments

DoD Chief Information Officer



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUL - 1 2021

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: DoD OIG Draft Report - Audit of the DoD Recruitment and Retention of the Civilian Cyber Workforce (D2020-D000CX-0032.000) Draft Report

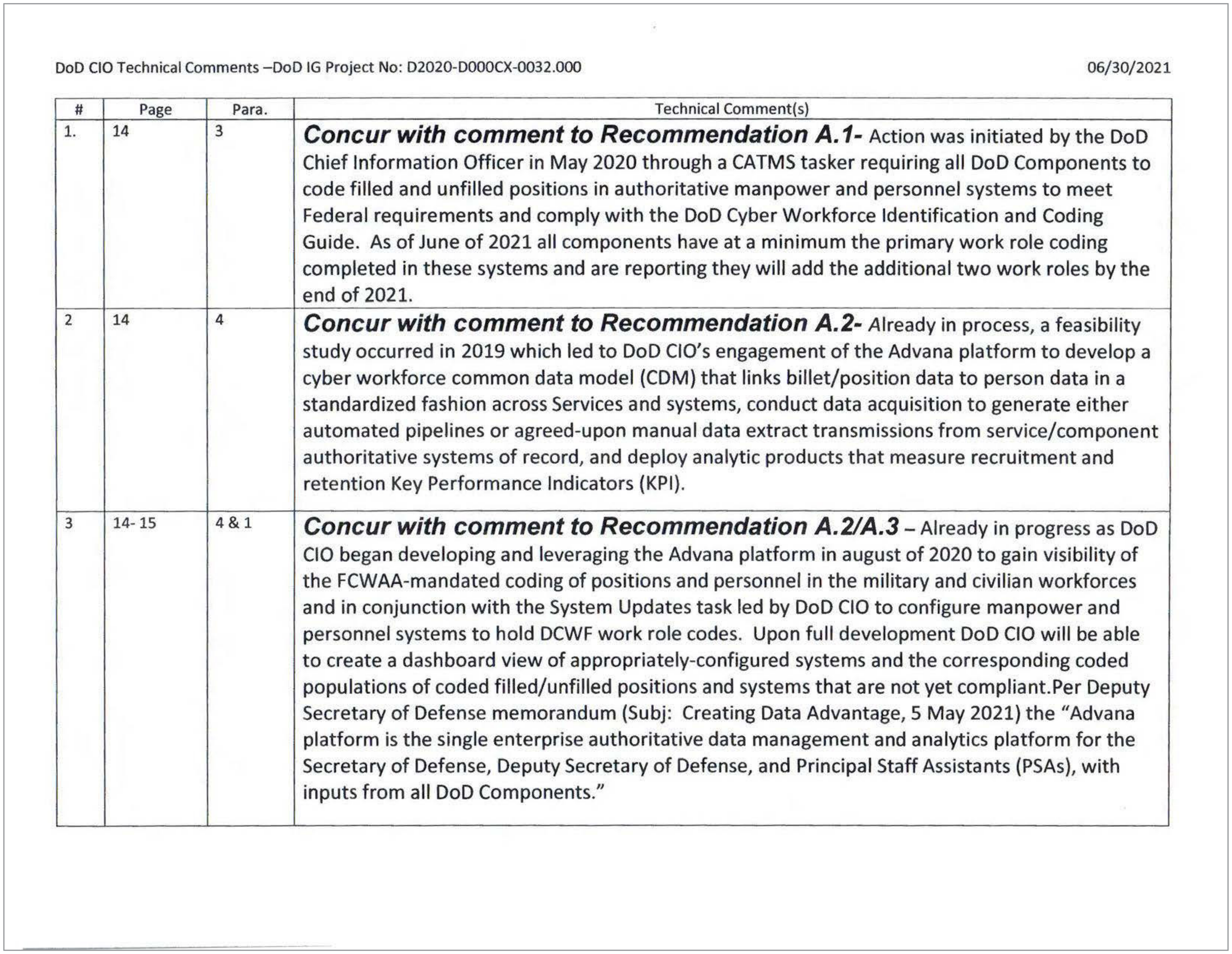
This memorandum and comment matrix are provided in response to your request of June 10, 2021, regarding the subject report. The DoD Chief Information Officer-(CIO) concurs with all recommendations. This response also includes a list of actions currently in progress to achieve the goals outlined in the recommendations.

My point of contact for this matter is [redacted], DoD CIO Cyber Workforce Division Chief (Acting), [redacted], or [redacted].

John B. Sherman
Acting

Attachment:
As stated

DoD Chief Information Officer (cont’d)



DoD CIO Technical Comments –DoD IG Project No: D2020-D000CX-0032.000 06/30/2021

#	Page	Para.	Technical Comment(s)
1.	14	3	***Concur with comment to Recommendation A.1-*** Action was initiated by the DoD Chief Information Officer in May 2020 through a CATMS tasker requiring all DoD Components to code filled and unfilled positions in authoritative manpower and personnel systems to meet Federal requirements and comply with the DoD Cyber Workforce Identification and Coding Guide. As of June of 2021 all components have at a minimum the primary work role coding completed in these systems and are reporting they will add the additional two work roles by the end of 2021.
2	14	4	***Concur with comment to Recommendation A.2-*** Already in process, a feasibility study occurred in 2019 which led to DoD CIO’s engagement of the Advana platform to develop a cyber workforce common data model (CDM) that links billet/position data to person data in a standardized fashion across Services and systems, conduct data acquisition to generate either automated pipelines or agreed-upon manual data extract transmissions from service/component authoritative systems of record, and deploy analytic products that measure recruitment and retention Key Performance Indicators (KPI).
3	14- 15	4 & 1	***Concur with comment to Recommendation A.2/A.3*** – Already in progress as DoD CIO began developing and leveraging the Advana platform in august of 2020 to gain visibility of the FCWAA-mandated coding of positions and personnel in the military and civilian workforces and in conjunction with the System Updates task led by DoD CIO to configure manpower and personnel systems to hold DCWF work role codes. Upon full development DoD CIO will be able to create a dashboard view of appropriately-configured systems and the corresponding coded populations of coded filled/unfilled positions and systems that are not yet compliant.Per Deputy Secretary of Defense memorandum (Subj: Creating Data Advantage, 5 May 2021) the “Advana platform is the single enterprise authoritative data management and analytics platform for the Secretary of Defense, Deputy Secretary of Defense, and Principal Staff Assistants (PSAs), with inputs from all DoD Components.”

Acronyms and Abbreviations

CES	Cyber Excepted Service
CIO	Chief Information Officer
CITEP	Cyber Information Technology Exchange Program
CySP	Cyber Scholarship Program
DCPAS	Defense Civilian Personnel Advisory Service
DA	Department of the Army
DAF	Department of the Air Force
DON	Department of the Navy
DCWF	DoD Cyber Workforce Framework
DCWS	DoD Cyberspace Workforce Strategy
DISA	Defense Information Systems Agency
EDIPI	Electronic Data Interchange Personal Identifier
FCWAA	Federal Cybersecurity Workforce Assessment Act
JFHQ-DODIN	Joint Force Headquarters-DoD Information Network
LoE	Line of Effort
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
OPM	Office of Personnel Management
USCYBERCOM	U.S. Cyber Command

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Whistleblower Protection

U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098