



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

8 April 2015

MEMORANDUM FOR DISTRIBUTION

Subj: CODING OF DEPARTMENT OF THE NAVY POSITIONS PERFORMING
CYBERSECURITY FUNCTIONS

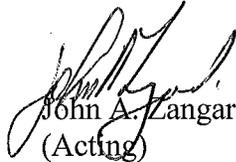
Ref: (a) United States Office of Personnel Management (OPM) Memorandum for Heads of
Executive Departments and Agencies, Subject: Special Cybersecurity Workforce
Project, of July 8, 2013

Encl: (1) Department of the Navy Civilian Cybersecurity Workforce Position, Personnel and
Position Description Coding Guide

Per reference (a), the Department of the Navy (DON) is required to code positions that perform cybersecurity work with Cybersecurity Data Element Codes established by the Office of Personnel Management (OPM). The OPM memo directs agencies to develop plans to complete initial position coding and then incorporate coding into agency hiring and position classification processes.

Together, the DON Chief Information Officer, DON Office of Civilian Human Resources, and Navy and Marine Corps civilian cybersecurity management personnel developed the responsibilities, requirements, and procedures necessary for FY 2015 implementation of OPM's direction. The result of this collaboration is enclosure (1), which provides guidance for DON Workforce Managers and Civilian Human Resources personnel for coding DON civilian positions performing cybersecurity work. The guide also includes instruction on incorporating the OPM Cybersecurity Data Element code into DON civilian position description documentation.

The DON point of contact for this matter is Mr. Chris Kelsall, who can be reached at chris.t.kelsall@navy.mil, or 703-695-1903.


John A. Zangardi
(Acting)

Distribution:
UNSECNAV
CNO
CMC
VCNO
ACMC
ASN RD&A
ASN M&RA

Subj: CODING OF DEPARTMENT OF THE NAVY POSITIONS PERFORMING
CYBERSECURITY FUNCTIONS

Distribution: (continued)

ASN FM&C

ASN EI&E

GC

DON/AA

DUSN Management

DUSN Policy

DNS

DMCS

NAVIG

JAG

OLA

CHINFO

AUDGEN

CNR

SAPRO

NCIS

CNO (DNS, N093, N095, N1, N2/N6, N3/N5, N4, N8, N9)

CMC (ACMC, ARI, M&RA, I, I&L, PP&O, C4, P&R)

COMPACFLT

COMUSFLTFORCOM

COMUSNAVEUR USNAVAF

COMNAVAIRSYSCOM

COMNAVRESFORCOM

COMNAVSEASYSYSCOM

CNIC

COMUSNAVCENT

USNA

COMFLT CYBERCOM

BUMED

COMNAVSAFECEN

NETC

COMNAVLEGSVCCOM

COMNAV SUPSYSCOM

COMUSNAVSO

COMNAV FACENCOM

NAVWARCOL

COMSPA WARSYSCOM

COMNAV SPECWARCOM

DIRSSP

BUPERS

COMNAVDIST

Subj: CODING OF DEPARTMENT OF THE NAVY POSITIONS PERFORMING
CYBERSECURITY FUNCTIONS

Distribution: (continued)

ONI

FLDSUPPACT

NAVPGSCOL

COMOPTEVFOR

COMMARCORSSYSCOM QUANTICO VA

COMMARFORCYBER

COMMARFOREUR

COMMARFORCOM

COMMARFORPAC

COMMARFORRES

COMMARFORSOUTH

COMMARSOC

CG MCCDC

CG MCRC

CG TECOM

Copy to:

DASN (CHR)

OPNAV N2/N6F3

NAVIDFOR N13IT

USMC DC, PPO, PLI

USMC HQMC C4, CY



DEPARTMENT OF THE NAVY

Civilian Cybersecurity Workforce Position, Personnel, and Position Description Coding Guide

25 March 2015

Department of the Navy
Chief Information Officer

Enclosure (1)

Department of the Navy Civilian Cybersecurity Workforce Position, Personnel, and Position Description Coding Guide

1. **Purpose.** This guidance is provided to ensure appropriate coding of civilian Cybersecurity Workforce (CSWF) positions, personnel, and position descriptions (PDs). It includes information on how to identify and categorize cybersecurity work, code positions, and submit coding information for inclusion in the Defense Civilian Personnel Data System (DCPDS). It also includes procedures for properly annotating civilian cybersecurity PDs, maintaining and modifying position and personnel Cybersecurity Data Element information, and reviewing Department of the Navy (DON) CSWF information to keep it current, complete and valid.

2. **Background.** The United States Office of Personnel Management (OPM) July 8, 2013 Memorandum for Heads of Executive Departments and Agencies directs Federal Agency cybersecurity, information technology and HR communities to build a statistical data set of existing and future cybersecurity positions in the OPM Enterprise Human Resources Integration (EHRI) data warehouse. This effort will support the President's goal of reducing CSWF gaps.
 - a. The memorandum directs agencies to use the National Cybersecurity Workforce Framework (NCWF) to define cybersecurity work.

 - b. The Cybersecurity Data Element standard in the OPM Guide to Data Standards (<http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf>) mirrors the cybersecurity work definitions of the National Initiative for Cybersecurity Education (NICE) framework.

 - c. The OPM memorandum directs agencies to:
 - (1) Review existing Federal positions that may be performing cybersecurity work with established position classification procedures and guidance in OPM's The Classifier's Handbook;
 - (2) Code all existing positions performing cybersecurity work with the Cybersecurity Data Element (all positions within the Information Technology Management 2210 Occupation series must be assigned a Cybersecurity Data Element code);
 - (3) Annotate cybersecurity position PDs with the Cybersecurity Data Element code;
 - (4) Submit coding information to the EHRI database. Department of Defense (DoD) information will be submitted to EHRI via DCPDS;
 - (5) Properly classify, maintain, and update all new and future positions performing cybersecurity work beginning in Fiscal Year 2015, including changes in the Cybersecurity Data Element Codes for positions currently classified; and,

(6) Assign the OPM Cybersecurity Data Element Code to positions in other occupational series to which cybersecurity work is assigned.

3. Status.

- a. The DON has completed the initial Series 2210 coding requirement and continues to review and assign the OPM Cybersecurity Data Element to positions in other occupations.
- b. The DON has begun an effort to annotate PDs for positions performing Cybersecurity work.
- c. The DON is establishing a process for maintaining and updating cybersecurity coding information in DCPDS.
- d. This guide provides initial direction to the PD and coding information management efforts.
- e. This guidance is applicable to DON Cybersecurity Workforce Managers, cybersecurity personnel, and to DON civilian HR personnel.

4. **Scope.** This guidance applies to all positions performing cybersecurity work regardless of civilian occupation series, including, but not limited to, the following occupation series:

- 2210 - IT Specialist
- 1550 - Computer Scientist
- 0332 - Computer Operation
- 0335 - Computer Clerk and Assistant
- 0390 - Telecommunications Processing
- 0391 - Telecommunications
- 0392 - General Telecommunications
- 1410 - Librarian
- 1411 - Librarian Technician
- 1412 - Technical Information Services
- 1420 - Archivist
- 1421 - Archivist Technician
- 0854 - Computer Engineering
- 0855 - Electronics Engineering

Figure 1 portrays the Cybersecurity Framework and associated OPM Cybersecurity Data Element codes.

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

DON Cybersecurity Workforce Model

Line of Operation	Category	Specialty Areas						
Department of Defense Information Networks (DoDIN)	Security Provision (60)	Information Assurance Compliance (61)	Software Engineering (62)	Enterprise Architecture (65)	Technology Demonstration (66)	Systems Requirements Planning (64)	Test and Evaluation (67)	Systems Development (63)
	Operate & Maintain (40)	Data Administration (42)	Info System Security Mgt (72)	Knowledge Mgt (43)	Customer & Tech Support (41)	Network Services (44)	System Administration (45)	Systems Security Analysis (46)
		RF/Teleport Operations (47)	Telephony/ Telecommunications Management (48)		Space Payload Operations (49)	Info Systems Security Operations (72)		
Defensive Cyber Operations (DCO)	Protect & Defend (50)	Computer Network Defense (CND) (51)	Incident Response (53)	CND Infrastructure Support (52)	Cyber Operational Planning (33)	Vulnerability Assessment & Mgt (54)	Cyber Threat Analysis (14)	
	Investigate (20)	Investigation (22)	Digital Forensics (21)					
Cyber Capability Support	Oversee & Govern (70)	Strategic Planning & Policy (75)	Security Program Mgt (74)	Education & Training (71)	Cybersecurity Program/Project Manager (80)	Cybersecurity Supervision, Management and Leadership (90)		

DON IT/CYBERSPACE EFFICIENCIES • ENTERPRISE ARCHITECTURE • EMERGING TECHNOLOGY • ENTERPRISE COMMERCIAL IT STRATEGY • CYBERSECURITY • CYBER/IT WORKFORCE INVESTMENT MANAGEMENT • CRITICAL INFRASTRUCTURE • INFORMATION SHARING • KNOWLEDGE & RECORDS MANAGEMENT • PRIVACY • NAVAL NETWORKS • ENTERPRISE SERVICES

Figure 1: NICE Framework; specific to the DON CSWF

5. **Applicability.** This guidance is to be used by DON Cybersecurity Workforce Managers and Civilian Human Resources personnel in developing, modifying, approving and maintaining civilian cybersecurity positions, PDs and personnel files. It is applicable to all CSWF positions, regardless of occupation.

6. **Responsibilities.**

a. Department of the Navy Chief Information Officer (DON CIO)

- (1) Serve as the DON Civilian Information Technology and Cyberspace Functional Community Manager.
- (2) Serve as the DON Office of Primary Responsibility (OPR) for the cybersecurity workforce.
- (3) In coordination with the Deputy Assistant Secretary of the Navy, Civilian Human Resources (DASN (CHR)), support development and use of procedures to ensure proper classification of DON civilian cybersecurity positions.
- (4) Provide oversight to validation of the establishment, modification and deletion of civilian cybersecurity positions.
- (5) Advise DON leadership of civilian cybersecurity workforce issues and gaps and provide recommendations for resolution.

b. Navy and Marine Corps Cybersecurity Workforce Offices of Primary Responsibility (OPR)

- (1) Serve as the civilian cybersecurity workforce leads for their respective Services.
- (2) Implement civilian cybersecurity position, personnel, and associated documentation processes and procedures in accordance with policy, procedures, and standards; including PDs.
- (3) Ensure Service cybersecurity management personnel (Information Systems Security Manager (ISSM), Cybersecurity Workforce Program Manager, and cybersecurity workforce managers) adhere to policy for the development, review, validation and submission of civilian cybersecurity workforce position establishment, modification and deletion procedures. This includes ensuring that cybersecurity management personnel coordinate with the proper HR personnel to ensure that requests at the Headquarters, Budget Submitting Office, and Office of Civilian Human Resources (OCHR) levels are made through the appropriate DON and Service approval processes.
- (4) Develop and implement Service-specific Cybersecurity Workforce policy and guidance.
- (5) Validate requirements and ensure proper documentation for the establishment, modification and deletion of civilian cybersecurity positions.
- (6) Continually review organization civilian CSWF coding in the Total Workforce Management System (TWMS) database. Coordinate with OCHR personnel to ensure DCPDS contains accurate and valid coding information.
- (7) Advise Service cybersecurity organizations and leadership regarding civilian cybersecurity workforce requirements, gaps, and recommended actions.

c. Information Systems Security Manager (ISSM)

- (1) Responsible for the organization's overall cybersecurity program.
- (2) Determine what civilian Cybersecurity Workforce positions have authorities, responsibilities and tasks requiring that assigned personnel be designated privileged users.
- (3) Review and validate requests for new civilian cybersecurity positions, and modification or deletion of existing positions.
- (4) Provide assistance to the Cybersecurity Workforce Program Manager (CSWF-PM) and cybersecurity managers regarding tasks and knowledge required for civilian cybersecurity positions.

- (5) Monitor the organization's CSWF program to ensure that it adheres to policy, guidance, and standards and report any discrepancies to the commanding officer.

d. Cybersecurity Workforce Program Manager (CSWF-PM)

- (1) Responsible for administration of the organization's CSWF Program.
- (2) Account for reporting, database management and overall effectiveness of the program at the organization and at subordinate organizations where appropriate.
- (3) Code civilian cybersecurity PDs in accordance with policy and guidance using the DON Cybersecurity Workforce Framework and OPM Cybersecurity Workforce data elements.
- (4) Request new civilian cybersecurity positions or modification or deletion of existing positions in accordance with established processes for approval of requests within the chain of command and HR organizations.
- (5) Collaborate with HR personnel to ensure that civilian cybersecurity PDs are complete and accurate and meet classification standards.
- (6) When advised that position and/or personnel changes have been made, validate that the information is accurately captured in the TWMS CSWF Module.
- (7) Continually review the organization's civilian CSWF coding in the TWMS CSWF Module.

e. Cybersecurity Managers/Supervisors

- (1) Collaborate with the organization's CSWF-PM to ensure the organization's civilian CSWF requirements are identified and documented.
- (2) Advise and collaborate with the CSWF-PM to ensure the organization's civilian CSWF positions are properly coded and updated.
- (3) Ensure that approved changes are recorded in PDs and local personnel records.
- (4) Advise and collaborate with the organization's CSWF-PM to ensure civilian CSWF PDs are accurate and complete. This includes an annual review of all of the organization's CSWF PDs.

f. DON Office of Civilian Human Resources

- (1) In coordination with DON CIO, establish and maintain policy, procedures and standards for coding civilian cybersecurity positions, personnel and associated documentation, including PDs.
- (2) In coordination with DON CIO, support development and use of procedures to ensure proper classification of DON civilian cybersecurity positions.

g. OCHR Operations Centers

- (1) Ensure that positions built within the DoD authoritative database, DCPDS, reflect the appropriate cybersecurity codes, as provided on the PD coversheet (OF-8 or equivalent).

7. Procedures.

a. Identifying and Documenting New Cybersecurity Positions

- (1) The Navy TWMS Module (<https://twms.navy.mil/login.asp>) shall contain all approved Navy CSWF position information and will use position and personnel Cybersecurity Data element information from the DoD authoritative database, DCPDS, for online reviews.
- (2) DON CSWF positions have been identified and assigned codes based upon NICE framework categories and specialty areas as detailed in Figure 1. OPM Cybersecurity Data Element codes are applied to all Federal civilian Cybersecurity positions.
- (3) Managers should review the tasks and knowledge, skills and ability (KSA) requirements documented on employee PDs and compare them to the descriptions associated with the assigned OPM Cybersecurity Data Element Code. If the code definition does not provide the level of detail needed, refer to the NICE framework available at <http://niccs.us-cert.gov/training/tc/framework> .
- (4) The OPM Cybersecurity Data Element code zero series (10, 20, 30, 40, 50, 60, 70, 80 and 90) map to the Categories in the Framework. The sub codes (e.g., 11, 12, 21, and so forth) equate to the Specialty Areas in the Framework. The sub codes 47, 48, and 49 are DON unique; when reporting to OPM, code 40 should be used in their place.
- (5) Managers shall amend or modify employee PDs as needed to reflect tasks and KSAs associated with the Cybersecurity Data Element Code. When a PD is amended or modified, it must be submitted through the classification review process to ensure position classification (assignment of pay plan, series, grade, and title) remains accurate.

- (6) DCPDS shall contain all approved DON Civilian CSWF position information.
- (7) All Civilian cybersecurity PDs shall include OPM Cybersecurity Data Element Codes on the PD coversheet (OF-8 or equivalent). The designated code will also be annotated on the DON Recruit Fill Form under Cybersecurity and provided with Requests for Personnel Action (SF-52) when applicable. PDs will be required for any position build modifications that require Cybersecurity code updates.
- (8) Requests for new CSWF positions must be validated by the organization's CSWF Program Manager (CSWF-PM) prior to entry into the manpower change process.
- (9) Requests for new positions must follow the approval process established by the organization's headquarters.
- (10) DON Cybersecurity positions are subject to USN and USMC Cybersecurity OPR review.
- (11) OPR review will follow Budget Submitting Office (BSO) review. The submitting office must provide justification with sufficient detail to support position establishment, modification, or deletion.
- (12) When approved by the OPR, cybersecurity code information will be entered into DCPDS by HR personnel upon submission of a completed DON Recruit Fill form and an updated PD. The established procedures of the servicing Operations Center must be followed (i.e., through a Request for Personnel Action (RPA) or through established corrective action procedures).

b. Modifying Cybersecurity Position Information

- (1) When an organization identifies the need to modify a civilian cybersecurity position, established procedures for updating DCPDS must be followed.
- (2) Requests for modification of DON CSWF positions must be validated by the organization's CSWF Program Manager prior to submission to the manpower information change process.
- (3) Managers shall review proposed PD task and KSA changes and match that information against the currently assigned OPM Cybersecurity Data Element Code. If sufficient differences from the previous "To" position to the proposed position exist, then review the tasks and KSA requirements documented on the proposed PD and compare them to the descriptions associated with the OPM Cybersecurity Data Element Code. If the code definition does not provide the level of detail needed, then the NICE framework available at <http://niccs.us-cert.gov/training/tc/framework> can be consulted for detailed information.

- (4) The OPM Cybersecurity Data Element code zero series (10, 20, 30, 40, 50, 60, 70, 80 and 90) map to the categories in the Framework. The sub codes (e.g., 11, 12, 21) equate to the Framework Specialty Areas. The sub codes 47, 48, and 49 are DON unique; when reporting to OPM, code 40 should be used in their place.
- (5) DON Cybersecurity positions are subject to Cybersecurity OPR review following BSO review. The submitting office must submit justification with sufficient detail to support position establishment, modification, or deletion.
- (6) When notified of approval by the OPR, the local command responsible for position classification shall update the PD coversheet (OF-8 or equivalent) with the new code. Pen and ink change is acceptable.
- (7) Once the PD has been updated with the approved code, the Cybersecurity Data Element Code information can be updated in DCPDS.
- (8) The command then submits all Cybersecurity Data Element Code modification and correction requests with the updated PDs to the servicing OCHR Operations Center, following all applicable procedures.

c. Processing Civilian Cybersecurity Personnel Information

- (1) All Civilian Cybersecurity Position recruiting and personnel actions shall follow established Civilian Human Resources guidance.
- (2) The OPM Cybersecurity Data Element Code shall be included on the PD coversheet (OF-8 or equivalent), and noted on the DON Recruit Fill Form or RPA, as appropriate.
- (3) CSWF personnel training and education information shall be documented in the personnel file in accordance with established DON Civilian Human Resources procedures.

d. Maintaining and Validating Cybersecurity Workforce Position Information

- (1) Quarterly, or more often if needed, the CSWF-PM will coordinate a review with OCHR to validate Cybersecurity position information. This will entail, at a minimum, developing a list of GS 2210 positions in DCPDS that do not have OPM Cybersecurity Data Elements assigned. If a position does not have a code assigned, the appropriate code will be determined by the Service OPR and submitted for entry in DCPDS and associated PDs.
- (2) DON CIO, the Navy and the Marine Corps will use the DON CSWF Module in TWMS to monitor civilian position status within TWMS. Any shortfalls or issues will be noted and resolved through the Service OPR and chain of command.