United States of America

BEFORE THE FEDERAL SERVICE IMPASSES PANEL

In the Matter of NATIONAL ASSOCIATON OF GOVERNMENT EMPLOYEES (NAGE), LOCAL R1-134 And NAVY, NAVAL UNDERSEAS WARFARE CENTER (NUWC), DIVISION OF BAVA SEA COMMAND, NEWPORT, RI	Case No. 22 FSIP 075

ARBITRATOR'S OPINION AND DECISION

This case, filed by the National Association of Government Employees (NAGE), Local R1-134 (Union) on August 1, 2022, is over negotiations with the Department of Navy, Naval Undersea Warfare Center, Division of Naval Sea Command, Newport, Rhode Island (NUWC or Agency) regarding changes in the Cyber Security Workforce (CSWF) Program. The parties are governed by a 2004-Collective Bargaining Agreement (CBA), which expired in 2007, but the terms remain in effect.

The Agency's mission is to research and develop underwater weapon systems. There are approximately 3,500 employees at NUWC. The NAGE Union represents approximately 618 Bargaining Unit employees. The negotiations with this Union will cover the working conditions of approximately 70 bargaining unit employees impacted by the change in the Cyber Security Workforce Program. This Union's impacted bargaining unit employees occupy primarily Technician and Information Systems (GS-2210) positions. The Union filed the request for Panel assistance in accordance with Section 7119 of the Federal Service Labor-Management Relations Statute (the Statute).[1]

Following the investigation of the Union's request for assistance in resolving the bargaining impasse over changes in the CSWF program, the Panel determined that the dispute over 19 remaining issues would be resolved through Mediation-

[1] 5 U.S.C. §7119.

Arbitration with the undersigned, Panel Member Edward Hartfield. The parties were informed that I would issue a binding decision to resolve the dispute if a settlement was not reached during mediation. Consistent with the Panel's procedural determination on October 16, 2022, I conducted a virtual mediation-arbitration proceeding with representatives of the parties. During the mediation phase, the parties agreed to explore settlement options to resolve the remaining matters. The parties were able to resolve some provisions successfully but remain in disagreement over the following provisions:

- Union 2/Agency 2
- Union 3
- Union 3.b
- Union 3.k
- Union 3.o
- Union 3.p
- Union 3.q.
- Union 3.r.
- Agency 2.d.
- Agency 2.l

Because the mediation portion of the proceeding failed to result in the voluntary settlement of these outstanding provisions, I am issuing a final decision resolving the parties' dispute over that matter in accordance with 5 U.S.C. §7119 and 5 C.F.R. §2471.11 of the Panel's regulations. In reaching this decision, I have considered the entire record, including post-hearing submissions by both parties.

BACKGROUND

The Federal Cybersecurity Workforce Assessment Act of 2015 requires that the head of each Federal agency shall take steps to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education's coding structure), and will execute on the requirements in the Federal Cybersecurity Workforce Assessment Act of 2015.

The parties began discussing implementing the Federal Cybersecurity Workforce Assessment Act of 2015 in 2017. However, the negotiations were held in abeyance pending the issuance of the Department of Defense (DoD) and Department of Navy (DoN) policies, including:

a. DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification (SECNAVINST 5239.20A, 10 Feb 2016)

b. DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual (SECNAV M-5239.2 dated Jun 2016)

c. DoN Memorandum of 26 May 2020 on Policy Updates to SECNAV M-5239.2

On December 16, 2021, the Agency provided the Union notice and an opportunity to bargain over policy changes, including the change to the Cyber Security Workforce certification and qualification requirements. The most impactful changes included not only changes to the mandatory certification/qualifications but also: mandatory training, mandatory condition of employment requirements, and language required for the Level Descriptor Addendum (also known as the position description under the Demonstration Personnel Project).

On January 24, 2022, the Union provided a counter-proposal. The parties engaged in negotiations over the proposals for four months. On May 6, 2022, the Agency requested mediation assistance. The parties engaged with a Federal Mediation and Conciliation Service (FMCS) Mediator in May 2022 and June 2022. The Mediator released the parties on July 20, 2022. On July 22, 2022, the Agency sent the Union notice of its intent to implement the changes. The Union requested the assistance of the FSIP.

ISSUES AT IMPASSE

On September 16, 2022 the Panel asserted jurisdiction over 19 remaining provisions. During the mediation, the parties reached an agreement on a number of issues. However, the following provisions remained at an impasse:

- Union 2/Agency 2
- Union 3
- Union 3.b
- Union 3.k
- Union 3.o
- Union 3.p
- Union 3.q.
- Union 3.r.
- Agency 2.d.
- Agency 2. l

While several provisions remain in dispute, the dispute comes down to a few disagreements: 1) the Union's proposals to include specific reference documents in the Agreement and 2) the duration of the Agreement.

Union Proposal 2

2. The Parties agree that the implementation of the Cyber Security Workforce shall be in accordance with the latest revision of the following listed documents (hereinafter references) and this MOU:

a. DoD 8570.01-M Information Assurance Workplace Improvement Program of 11/10/2015

b. DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification (SECNAVINST 5239.20A, 10 Feb 2016)

c. DoN Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual (SECNAV M-5239.2 dated Jun 2016)

d. DoD Cyber Workforce Identification and Coding Guide Version 1.0, dated 31 Aug 2017

e. DoN Memorandum of 26 May 2020 on Policy Updates to SECNAV M-5239.2

Union Argument for Proposal 2

The Union argues that it is critical that the Union stewards and the bargaining unit employees have a clear understanding of the "Baseline Instructions" that the Agency has agreed to and is, therefore, required to adhere to in implementing the requirements of the Cyber Security Workforce program. By including the specific versions in the Agreement, the Union representatives and the impacted employees don't have to guess which policies apply. The Union recognizes that those policies may be updated over time (i.e., "[t]he Parties agree that the implementation of the Cyber Security Workforce shall be in accordance with the latest revision of following listed documents" (Union Proposal 2)). However, the Union's proposed language fails to provide access to changes in the applicable policies. That language could be improved by providing a link to the latest, applicable version of the policies.

Agency Proposal 2

2. The Parties agree that the implementation of the Cyber Security Workforce shall be in accordance with the latest revision of DoD and DoN policies regarding the CSWF/Cyber IT workforce. These documents will be posted and available to employees on the command intranet (currently, https://wiki.navsea.navy.mil/pages/viewpage.action?spaceKey=

NPTCYBERWF&title=NUWCDIVNPT+Cybersecurity+Workforce+Home+Page). If any of these documents change, Management will provide copies of the documents to the Union. If any changes to Agency policy impact working conditions, Management agrees to provide reasonable notice and opportunity to negotiate these changes in accordance with the labor statute.

Agency Argument for Proposal 2

The Agency agrees that the employees need a clear understanding of what is required of them, and the Agency needs to be able to be clear in executing the workforce requirements, including qualifications, positions descriptions, required training, duration of the training, certifications, continuous learning requirements, and other mission program areas in accordance with relevant DoD/DoN CSWF policies. However, the Agency argues that by not simply linking but actually citing the applicable policies that were in place at the time of the negotiations, there may be restrictions and issues in the future. The workforce would be limited by not having access to the changing directives. The Agency proposal would provide access to an online link to the latest policies. The Agency recognizes that policy changes may trigger a bargaining obligation. The Agency's proposal can be improved by ensuring that the policy, accessible by the bargaining unit through the online link, has been subject to collective bargaining with the Union and, therefore, applies to the bargaining unit.

Opinion for Union Proposal 2/Agency Proposal 2

Both parties agree that the workforce needs to know and have ready access to the current policies that apply to the CSWF Program. The Agency's argument is that citing the policies that were in place at the time of negotiating the Agreement would potentially limit the Agency's implementation of the policies. I disagree. The bargaining unit employees, their representatives, and their supervisors should have a clear understanding of the starting instructions for the CSWF Program, including qualifications, position descriptions, required training, duration of the training, certifications, and continuous learning requirements; all included in the relevant DoD/DoN CSWF Program policies. Both parties agree that any changes in the instructions that apply to the CSWF Program will be subject to collective bargaining with the Union and thereafter available to the workforce. The Agency's language that provides an online link ensures access to the currently applicable policies.

Union Proposals 3, 3(b), 3(k), 3(o), 3 (p), 3 (q), 3(r)

3. As to matters pertaining to NAGE R1-134 bargaining unit members, the Agency agrees to comply with all the requirements of References (a) through

(e), in the implementation of the Cyber Information Technology/Cybersecurity Workforce (Cyber IT/CSWF).

3. b. It is recognized by the parties that reference (b) defines the specialty area and work role cyber knowledge, skills, and abilities (KSAs) required to perform the Cyber IT/CSWF functions at differing proficiency levels, and the Cyber IT/CSWF workforce is identified based upon the extent of their role in Cyber IT and Cyber Security work. These levels are 1. Basic, 2. Intermediate, and 3. Advanced.

3. k. Required Cyber IT/CWSF qualification and corresponding proficiency levels, contained in reference (a) through (e), shall be posted on the NUWCDIVNPT Intranet or similar site, which is accessible to employee Union officials and bargaining unit members.

3. o. Each DON Cyber IT/CSWF position must be identified with a Category, Specialty Area, and Proficiency Level. Categories and Specialty Areas are shown in Figure 2 of SECNAV M-5239.2 June 2016 23 Chapter 3

3. p. The proficiency levels incorporated into the DON qualification framework include:

(a) Entry/Apprentice –Basic understanding of computer systems and related cybersecurity software and hardware components.

1. Civilian Grades 5, 7, and 9 SECNAV M-5239.2 June 2016 Chapter 3

(b) Intermediate/Journeyman –Working knowledge and application of IS and security operational characteristics for various computer platforms, networks, software applications, and OSs.

1. Civilian Grades 9, 11, 12

(c) Expert – Advanced application and mastery of IS, plans, and functions, and is responsible for the Management of complex projects and initiatives with a large scope.

1. Grades 13 and above.

3. q. The DON workforce is identified based on the extent of their role in Cyber IT and cybersecurity work. The specific workforce classifications are:

(a) Authorized User: Requires general computer skills and a baseline understanding of cybersecurity to conduct work that is not IT and/or cybersecurity focused. This is the general DON workforce - military, civilian, and contractor.

(b) Enhanced User: Authorized Users who require detailed knowledge of Cyber IT and/or cybersecurity to support work in the development, maintenance, and operations of multiple DON systems, including weapons, tactical, electronic and electrical services, navigation, and engineering. This personnel requires advanced knowledge of Cyber IT/CS, but their knowledge and abilities are centered on their professional area.
(c) Core Cyber IT/CS User: Authorized Users who require KSAs in the technical and managerial aspects of Cyber IT/CS. This group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network-centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and IS.

3.r. The agency is obliged and will follow the terms and conditions of this MOU and the references listed in this MOU.

Union Argument for Proposals 3, 3(b), 3(k), 3(o), 3 (p), 3 (q), 3(r)

The Union made the same arguments that it did for Proposal 2. The Union argues that these references need to be in the Agreement for clarity on the baseline of the CSWF program and requirements. While these same references are addressed in Proposal 2, the Union specifically calls out subsections of these policies in the sub-parts of Proposal 3 because of the bargaining unit's interest in those matters in particular: KSAs/qualifications, proficiency levels, and roles.

Agency Argument regarding Union Proposals 3, 3(b), 3(k), 3(o), 3 (p), 3 (q), 3(r)

The Agency made the same argument as it did for Proposal 2. The Agency argues that the references should not be included in the Agreement because the Agency should not be held to reference that may no longer be applicable or used by the DoD or DoN in managing the CSWF Program. The Agency offers an argument that including the references and stating that the Agency will comply with all of the requirements of those references is non-negotiable.

Opinion regarding for Union Proposals 3, 3(b), 3(k), 3(o), 3 (p), 3 (q)

The inclusion of the references is addressed in Proposal 2. The employees will find the specifics within those references online through the intranet link. The

Union may want to also prepare a reference guide for its members to facilitate links to specific areas of interest for the bargaining unit employees. The Union is ordered to withdraw its Proposals 3, 3(b), 3(k), 3(o), 3 (p), 3 (q), and 3 (r).

Agency Proposal 2(d)

> 2. d. Each unit member, who is a member of the Cyber IT/CSWF, shall have their Level Descriptor Addendum (LDA) position identified with a specialty area(s), work role code(s), proficiency level(s), credentialing requirement, and continuous learning requirements. An electronic copy of the LDA will be sent to the employee with the appointment letter.

Opinion regarding Agency Proposal 2(d)

During the mediation, the parties agreed to the Union's Proposal 3.e and agreed to remove the Agency's Proposal 2.d. The Agency is ordered to withdraw its Proposal 2.d.

Agency Proposal 2(l)

> Agency 2. l. This agreement is binding upon both parties. The agreement can be renegotiated or terminated at the end of two (2) years or anytime thereafter by either party with a thirty (30) day notice to the other.

Agency Argument regarding Agency Proposal 2(l)

The proposed language provides for renegotiating this Agreement or terminating the Agreement at the end of 2 years or anytime thereafter by either party with a 30-day notice. The Agency provided no explanation or argument regarding the duration of the Agreements under the parties' current collective bargaining agreement or the reasons for treating this Agreement differently than what is provided under the CBA. With no compelling reason offered for this language, the Agency is ordered to withdraw its Proposal 2. l.

DECISION

Having carefully considered the arguments and evidence presented in this case, as the Statute requires, I hereby order the parties to adopt the following language in their agreement regarding the CSWF program:

2. The Parties agree that the implementation of the Cyber Security Workforce shall be in accordance with this MOU and the latest revision of DoD and DoN policies regarding the CSWF/Cyber IT workforce, including:

a. DoD 8570.01-M Information Assurance Workplace Improvement Program of 11/10/2015
b. DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification (SECNAVINST 5239.20A, 10 Feb 2016)
c. DoN Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual (SECNAV M-5239.2 dated Jun 2016)
d. DoD Cyber Workforce Identification and Coding Guide Version 1.0, dated 31 Aug 2017
e. DoN Memorandum of 26 May 2020 on Policy Updates to SECNAV M-5239.2

The applicable policies will be posted by Management and available to employees on the command intranet (currently, https://wiki.navsea.navy.mil/pages/viewpage.action?spaceKey=NPTCYBERWF&title=NUWCDIVNPT+Cybersecurity+Workforce+Home+Page).

If any applicable policies change, Management will provide copies of the documents to the Union. If any changes to Agency policy impact the working conditions of the bargaining unit, Management agrees to provide reasonable notice and opportunity to negotiate these changes in accordance with the labor statute.

The posting of changes to applicable policies on the command intranet will be made once collective bargaining obligations have been met.

Edward Hartfield
Panel Member

November 23, 2022