UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD
REGION 32

KAISER FOUNDATION HEALTH PLAN, INC.

Employer

and

Case 32-RC-367739

INTERNATIONAL UNION OF OPERATING ENGINEERS, STATIONARY ENGINEERS, LOCAL 39, AFL-CIO

Petitioner

DECISION AND DIRECTION OF ELECTION

Kaiser Foundation Health Plan, Inc. (Employer) operates various hospitals and clinical medical facilities throughout the country in Washington state, the Northwest (mainly Oregon), Northern California, Southern California, Hawaii, Colorado, Georgia, and the Mid-Atlantic region of Washington, D.C., Maryland, and Virginia. On June 17, 2025,[1] International Union of Operating Engineers, Stationary Engineers, Local 39, AFL-CIO (Petitioner or Union) filed a petition (Petition) under Section 9(c) of the National Labor Relations Act (the Act) seeking to represent a proposed unit of six (6) IoMT Leads, Clinical Systems Engineers – IoMT Specialists, and Biomedical Engineering Chief Engineers at the Employer's Northern California facilities.

A hearing officer of the National Labor Relations Board conducted a hearing in this matter by videoconference on July 1, and the parties orally argued their respective positions prior to the close of the hearing.[2] The hearing addressed three timely raised issues. First, whether the job classifications in the proposed unit are guards under Section 9(b)(3) of the Act, as the Employer contends; second, whether the petitioned-for unit, limited to employees at the Employer's Northern California facilities is an appropriate unit for bargaining, or whether the unit also must include all employees in these job classifications nationwide, as the Employer contends; the third issue is the election mode.

As explained below, based on the record and relevant Board law, I find that the job classifications in the unit are not guards under Section 9(b)(3) of the Act, and that the petitioned-for unit is an appropriate unit. Moreover, based on the scattered nature of the unit, I find that a mail-ballot election is the most appropriate election mode in this case.

[1] All dates refer to 2025, unless otherwise specified.
[2] The Employer submitted a pre-hearing brief and post-hearing memorandum of points and authorities.

I. THE EMPLOYER'S OPERATIONS

a. General Operations

The Employer is a healthcare provider with hospitals and clinical medical facilities throughout the country, mainly concentrated in California. The Employer has organized its operations into separate geographic regions. Those regions consist of: Washington state (0 hospitals, 36 medical offices), the Northwest region mainly covering Oregon (2 hospitals, 52 medical offices), Northern California (21 hospitals, 209 medical offices), Southern California (15 hospitals, 197 medical offices), Hawaii (1 hospital, 23 medical offices), Colorado (0 hospitals, 33 medical offices), Georgia (0 hospitals, 27 medical offices), and the Mid-Atlantic region of Washington, D.C., Maryland, and Virginia (0 hospitals, 45 medical offices).[3] The record shows that the Employer sometimes refers to these regions as Northern California, Southern California, and Markets Outside California (MOC). The record does not reflect exact distances, but facilities are in some cases thousands of miles from one another across the country. In each of the parties' proposed units, the employees work remotely from home and do not have assigned offices, but the Employer organizes them according to the regions described above.

Each of the Employer's hospital and clinical medical facilities houses medical equipment and devices used to treat, diagnose, or monitor patients. The "Internet of Medical Things" (IoMT) includes any of those devices in the healthcare delivery organization that needs to be connected to the Employer's network. These devices are distinct from laptops, desktop computers, and other traditional computing tools that IT can control and update remotely. The record shows that they typically include various layers of specialized and proprietary software on top of commonly-used software applications. Across all markets, the Employer has approximately 360,000 pieces of IoMT equipment, 150,000 of which are actual medical devices. This equipment comes from 1,600 individual vendors with multiple device models from each vendor.

b. Organizational Structure

Multiple teams sit under the Employer's Healthcare Technology Management (HTM) organization, headed by Vice President Mark Manning. The largest resource allocation of the HTM umbrella organization's staff goes toward keeping medical equipment safe, maintained, and ready for patients and members to use, in compliance with accreditation standards that vary by state. Under the HTM organization sit five categories of work: 1) medical equipment planning (source and purchase new equipment); 2) life cycle asset planning/technology coordination group (planning for replacement of each device); 3) service delivery (largest group, focused on maintaining equipment through preventive and corrective maintenance); 4) HTM cybersecurity; and 5) Nuvolo enterprise asset management (software used across the enterprise).

The fourth subset mentioned above, the HTM Cybersecurity unit, is headed by Executive Director Kris Kline. The HTM Cybersecurity unit includes multiple sub-teams categorized in the Employer's organization chart by director: three operations teams, one Cyber Risk Defense team managed by Senior Manager Amy Purvis, and Applications Support managed by Director Sean

[3] Facility counts listed in chart, "KP Scope of Edge Devices by Market", Employer Ex. 2.

Enners. Under Director Enners sits another level of management, including Program Management Manager Bernadette O'Doherty.

O'Doherty manages the three IoMT Cybersecurity Leads who oversee all of the approximately 20 workers categorized as IoMT Specialist – Cybersecurity. O'Doherty also directly manages multiple data analysts who analyze cybersecurity threats as they are identified by the separate Cyber Risk Defense team. IoMT Cybersecurity Field Team Specialists are organized under Team Leads according to their geographical location. The Lead for Northern California is Greg Marcisz, and the record shows that Northern California Specialists report only to Marcisz, not to any other lead, and Marcisz then reports to O'Doherty. The equivalent Lead for Southern California region is Rex Andrade, and then all other regions, called Markets Outside California (MOC) are under MOC IoMT Cybersecurity Field Team Lead Andrew Whittier. The petitioned-for unit of Northern California regional employees consists of 5 IoMT Cybersecurity Field Team Specialists and 1 Lead. The Employer's proposed nationwide unit consists of 20 IoMT Cybersecurity Field Team Specialists. The Employer seeks to exclude Leads from its proposed unit, and I decided to defer the issue to post-election proceedings because Leads constitute less than 20% of both the petitioned-for and Employer's proposed unit.

Hiring of the IoMT Cybersecurity Field Team

Multiple Employer managers testified that the IoMT Cybersecurity Field Team came about because after cybersecurity threats and vulnerabilities were located within the Employer's IoMT by a separate team sitting under a separate director, there was no team to implement the necessary fixes and apply prescribed controls. Initially the Employer hired contractors to perform such work, but between October 2024 and December 2024, it hired employees directly to do this work full time as an internal team, the IoMT Cybersecurity Field Team. Currently, all IoMT Cybersecurity Security Field Team employees in all regions are full-time, directly employed by the Employer. The Employer started this hiring nationwide in October 2024 and finished by hiring one employee in Georgia and the last of the petitioned-for Northern California employees in December 2024. This permanent hiring of Northern California IoMT Cybersecurity Field Team Specialists was managed by Northern California IoMT Cybersecurity Field Team Lead Greg Marcisz. The Record shows that Marcisz would first obtain verbal approval for a hiring request from Vice President Mark Manning. Marcisz was then responsible for submitting hiring requests via the Employer's HR system, scheduling interviews, and discussing candidates with Program Management Manager Bernadette O'Doherty and Director Sean Enners to determine whether the candidate was a fit for the team. IoMT Cybersecurity Field Team Lead Greg Marcisz had the final say in Specialist selection, and the Employer's nationwide HR team made the offers. The record is silent regarding the hiring process in other regions.

c. Workflow

Threat identification and analysis

Before assignments reach the IoMT Cybersecurity Field Team, at least two separate teams in the HTM organization are responsible for the intake, analysis, and working with the device manufacturer or vendor to identify security gaps or security requirements. Initially, notifications

about cybersecurity threats generally come to the Employer via an external National Vulnerability Database, fielded for intake by the Cyber Risk Defense team under Senior Manager Amy Purvis. Employees who sit under Manager of Program Management Bernadette O'Doherty then analyze the threats assigned to them by Cyber Risk Defense.

Application of controls

Only after two other teams identify and analyze the security threats and choose the appropriate controls does the HTM organization then assign to the IoMT Cybersecurity Field Team the task of applying controls or otherwise resolving the issue in the manner prescribed by the teams performing the threat analysis work. The assignment, based on the location of the device(s), goes to an IoMT Cybersecurity Field Team Lead to assign the work to Specialists in that Lead's geographic region. Field Team members visit sites in their region alone or with others assigned to the same region, and they work individually on devices. The IoMT Cybersecurity Field Team also does some controls testing on devices.

The proposed bargaining unit applies controls related to connected medical equipment, security and pharmacy equipment. This includes devices that cannot be managed remotely the way a typical IT department might deploy traditional software updates. The connected medical devices typically do not contain what in IT are referred to as "agents", species of software on a computer or server that allows IT to apply changes overnight, off cycle, during a device shutdown, etc. Here the HTM cybersecurity unit often must physically go to each device in question to deploy a device or change. VP Manning analogized the IoMT Cybersecurity Field Team's work to constantly plugging holes in a dam and described the work as maintenance and regular cybersecurity hygiene. The controls applied by the team include things like upgrading software applications, applying patches, shutting off communication ports, applying specific credentialing to protect a device by limiting which users can access it, and various configurations and administration-type screens. Beyond medical devices, the unit is trained and capable of working on other connected devices such as controls on elevators, HVAC systems, and security cameras. IoMT Cybersecurity Team members travel to sites within their assigned regions to do physical tasks when necessary.

d. Travel

IoMT Cybersecurity Field Team Specialists work on devices in other regions infrequently and in a handful of contexts. Without traveling, they may use network tools to identify devices during inventory management exercises and liaise with manufacturers to ensure accurate records, which the Employer's witness identified as inventory maintenance. Every member of the IoMT Cybersecurity Field Team receives training on the same software tools. All leads attend two weekly meetings, and all specialists join the leads for Friday weekly meetings to review organizational announcements, new work coming, comment on existing work, and hear guest speakers or trainers. The team members also utilize Microsoft Teams chat to communicate, but the evidence did not show how often this occurs. There are one to two "state of the union" meetings where the teams discuss goals. Onboarding training is done across markets, and the practice of "reverse inventory", tracking devices that show up on the network but are not listed in inventory, necessarily occurs across markets. Specialists can also handle work order tickets for devices in other markets, but the record does not show how often this occurs.

Employer testimony about travel was conflicting. First a witness testified that it was voluntary, and no member of the team had ever been compelled by the Employer to travel to another region. Later the same witness stated that travel has always been a requirement of the job. Evidence showed the petitioned-for bargaining unit, the IoMT Cybersecurity Field Team, fixes vulnerabilities in two ways: 1) the routine implementation of proactive security measures identified by other teams, and 2) what Employer witnesses variously referred to as "break-the-glass" or "zero-day" exigent circumstances with security vulnerabilities needing to be addressed as quickly as possible, in a matter of hours. Witnesses testified it is in those "break-the-glass"/"zero-day" scenarios when IoMT Field Team Members travel to other markets. The evidence showed that there have only been six cross-market travel events or projects: two trips to the Mid-Atlantic states, one or two trips to Hawaii, Colorado, and the Northwest. When employees did travel, they still worked independently of each other, with one person assigned to each device or with individuals working on different floors of the same facility. There was no evidence that any IoMT Specialists based outside California or in Southern California ever traveled to Northern California to do work. The evidence shows that the most recent "break-the-glass" scenario requiring travel occurred sometime before the inception of the team in December 2024. The travel described in pertinent emails all occurred while the team was comprised of contractors and the full-time positions in the proposed bargaining unit did not yet exist. No employee has permanently transferred from one region to another on the IoMT Cybersecurity Field Team.

e. Working conditions

Members of the IoMT Cybersecurity Field Team nationwide all have the same employee handbook, same benefits, 8 a.m. to 5 p.m. working hours in their respective time zones in all regions, relatively similar pay, but with geographic adjustments, and use the same tools to work. When Northern California IoMT Cybersecurity Field Team Specialists make sick day or PTO requests into the HR system, those requests are reviewed or denied by Lead Greg Marcisz. Lead Rex Andrade performs that role for Southern California Specialists, and Lead Andrew Whittier for the Markets Outside California.

f. Guard indicia

The evidence shows that IoMT Cybersecurity Field Team Specialists and Leads do not engage in surveillance of coworkers. When the IoMT Cybersecurity Field Team deploys controls on-site, they do not direct other employees, but rather they must work around clinical staff schedules. An Employer witness testified that the IoMT Cybersecurity Field Team cannot disrupt clinical operations and cannot ask a patient to reschedule an appointment so the team can work on a device. The IoMT Cybersecurity Field Team does "credential management" to ensure that default passwords on devices are changed, but there is no direct communication or training that the team is responsible for administering to clinical staff around cybersecurity. The IoMT Cybersecurity Field Team does not have a special responsibility to report infractions of password or other security policies beyond what all the Employer's employees are expected to do as part of the Employer's "speak-up culture."

Unit members do not wear guard-type uniforms or display other indicia of guard status. They do not carry weapons, handcuffs, or other physical security devices. The Employer has a separate physical security team with distinct uniforms and distinct guard badges. An Employer witness confirmed that when at its facilities, the IoMT Cybersecurity Team members have badges with their photos and names on them identifying them as Kaiser employees, but the badges do not identify them as guards, nor do they wear uniforms.

The IoMT Cybersecurity Field Team does not investigate internal cybersecurity threats posed by internal Kaiser employees. The Employer has other teams under Information Technology (IT) that conduct threat analysis and security forensics. The IoMT Cybersecurity Field Team does not monitor who accesses medical devices, activate or deactivate security devices or systems, or access patients' private health information. They do not get fingerprinted or photographed upon hire, but they do undergo drug testing and background checks standard to all the Employer's employees. They do not provide physical security for the Employer's facilities.

Finally, IoMT Cybersecurity Field Team Leads and Specialists are not expected to help safeguard the Employer's facilities and property if other employees go on strike.

II. ANALYSIS

A. The IoMT Cybersecurity Field Team Specialists and Leads are not Guards under Section 9(b)(3) of the Act.

Section 9(b)(3) of the Act prohibits the Board from finding a unit appropriate for the purpose of collective bargaining if it includes, together with other employees, guards that enforce rules against employees and others designed to protect the employer's property or for the protection and safety of those on the employer's premises. At issue here is whether the Employer's IoMT Cybersecurity Field Team Specialists and leads are guards under Section 9(b)(3).

In determining whether employees are guards, the Board looks at factors "typically associated with traditional police and plant security functions, such as the enforcement of rules directed at other employees; the possession of authority to compel compliance with those rules; training in security procedures; weapons training and possession; participation in security rounds or patrols; the monitor and control of access to the employer's premises; and wearing guard-type uniforms or displaying other indicia of guard status." *Boeing Co.*, 328 NLRB 128, 130 (1999). The Board has found that employees are statutory guards where they, for instance, wear a distinctive uniform and identification badge, carry a two-way radio to stay in constant communication with one another, and regularly enforce rules against patrons and staff in order to protect the employer's facility. *Madison Square Garden*, 333 NLRB 643, 645 (2001).

Although the Board uses the phrase "traditional police and plant security functions," employees need not wear uniforms, carry weapons, or receive special training to be considered guards. Nor does indicia of guard status such as the use of a guard/security related job title alone

confer guard status. *Ford Motor Co.*, 116 NLRB 1995, 1997 (1956). Rather, the Board has found employees to be guards if they have a significant, versus minor or incidental, role in monitoring and controlling access to the employer's premises or property, even if they do not have authority to independently enforce the rules. *Rhode Island Hospital*, 313 NLRB 343, 347 (1993) (security officers, traffic control guards, and security dispatchers were statutory guards where they protected the employer's property and the safety of persons on the property by regularly checking the premises and were administratively placed within the security department). In *Wackenhut Corporation*, 196 NLRB 278, 278-279 (1972), the Board found employees to be guards even where they "do not themselves have the power of police to ultimately determine and compel compliance by violators," as long as they possess and exercise responsibility to observe and report infractions. See also, *Wright Memorial Hospital*, 255 NLRB 1319, 1320 (1980) (ambulance department employees were guards where they made regular hospital rounds searching for fire, theft, vandalism, unauthorized personnel, and to make sure doors were locked, but could only report detected infractions to the department head); *Crossroads Community Correctional Center*, 308 NLRB 558, 561 (1992) (employee employed as a correctional counselor was a guard because in monitoring entrance to the employer's work release facility, and searching visitors and residents for contraband, the employee enforced against employees, residents, and other persons rules to protect the safety of persons on the employer's premises and keep unauthorized persons off the premises). Thus, employees are guards if they are "directly responsible for being alert to *any* incident, situation, or problem which needs responsive action and for reporting such incidents to the proper authorities." *Rhode Island Hospital*, 313 NLRB at 347.

Turning to the *Boeing* indicia:

The petitioned-for unit does not engage in the enforcement of rules directed at other employees, with the exception of assisting clinical employees, if needed, in changing default equipment passwords. The record showed that this is not a core job responsibility, and the petitioned-for unit is not expected to communicate directly or train other employees regarding changing default passwords. Further, the IoMT team does not possess the authority to compel compliance with those rules. The petitioned-for unit does not engage in weapons training or participate in security rounds or patrols, nor does it carry any physical or virtual weapons, security devices, or handcuffs.

The Employer raises the issue that technology has evolved and urges the Region to look at these facts in the current context. When cybersecurity is analogized with physical security to the extent possible, the facts nevertheless demonstrate that the virtual "security patrol" in this case happens elsewhere in the organization and threat management originates with an external vendor database. In contrast with the employees the Board found to be guards in *Wright Memorial*, *Rhode Island Hospital*, infra., IoMT Cybersecurity Field Team Leads and Specialists are not responsible for being alert to or reporting incidents. The Employer also cites *MGM Grand Hotel,* 274 NLRB 139 (1985) for the premise that employees were found to be guards

who were monitoring and reporting. Additionally, the Employer points to *PECO Energy Co.,* 322 NLRB 1074, 1083 (1997), stating that, "the Board found that a janitor who performed cleaning and maintenance work could be considered a guard because the employer assigned him additional security related duties." In *PECO Energy Co.*, the employee assigned to the formal job title of janitor was epileptic and could consequently no longer perform his janitorial duties at the plant, so he was assigned to the guard house. *Id*. Besides keeping the guard house clean, this employee's duties were the same as those of a guard formerly provided by an outside contractor: monitoring security cameras, operating motorized security gates and entrances, checking people into the property, and reporting infractions. *Id*. The employee was also meant to investigate and report suspicious situations to a supervisor. *Id*. For these reasons, the *PECO Energy Co*. example is not on point with the facts at hand. Finally, the Employer cites *Bellagio, LLC v. NLRB*, 863 F.3d 839 (D.C. Cir. 2017). There again the work involved surveillance and rule enforcement by training others to use the surveillance equipment, *Id*., unlike the IoMT Cybersecurity Field Team.

There are other teams under HTM who conduct this patrolling and reporting. Notably, the Employer has a team called Cyber Risk Defense that sits under a different manager than Applications Support Director Sean Enners. The Cyber Risk Defense team fields the threats from an external database, another team analyzes what to do, and then finally the IoMT Cybersecurity Field Team implements the patches and controls as instructed by those employees who operate more like guards elsewhere in the organization. Along the same vein, the petitioned-for unit also does not monitor and control access to the Employer's premises, including access to the IoMT.

Unit members do not wear guard-type uniforms or display other indicia of guard status. In fact, the Employer has a separate physical security team with distinct uniforms and guard badges. An Employer witness confirmed that when at its facilities, the IoMT Cybersecurity Team members have badges with their photos and names on them identifying them as Kaiser employees, but the badges do not identify them as guards, nor do they wear uniforms. In another case cited by the Employer, employees who did not wear uniforms were found to be guards due to the security functions they performed. However, again in contrast to the present case, those employees were found to, "possess and exercise responsibility to observe and report trespass infractions," *Allen Services Co.*, 314 NLRB 1060, 1062 (1994). The IoMT Cybersecurity Field Team is not engaged in the monitoring and reporting that crucially informed the decision in *Allen Services Co.* and the other cases relied upon by the Employer.

The petitioned-for unit does regularly go through training in security procedures, but these are related to software used to track device inventory and apply controls to those devices. This training in security procedures does not involve monitoring or reporting threats.

Taking the entirety of the record into consideration and viewing this question through a modern-day lens, I have determined that the IoMT Cybersecurity Field Team Leads and Specialists are not guards under Section 9(b)(3) of the Act.

B. The IoMT Cybersecurity Field Team Specialists and Leads in the Employer's Northern California Region Share a Distinct Community of Interest from IoMT Cybersecurity Field Team Specialists and Leads in Other Regions.

While the petitioned-for employees work remotely from their homes, they also regularly perform work at the Employers' various facilities in their respective geographic regions. At issue is whether the petitioned-for multi-facility Northern California regional unit is appropriate, or if the Northern California employees share a distinct community of interest apart from the nationwide unit proposed by the Employer.

"In determining whether a petitioned-for multifacility unit is appropriate, the Board evaluates the following factors: employees' skills and duties; terms and conditions of employment; employee interchange; functional integration; geographic proximity; centralized control of management and supervision; and bargaining history.' *Laboratory Corp. of America Holdings*, 341 NLRB 1079, 1081-1082 (2004). An appropriate multifacility unit is one that has a 'distinct' community of interest from the excluded facilities. Id. at 1082; see also *Acme Markets, Inc.*, 328 NLRB 1208, 1209 (1999). It is well settled that a petitioned-for unit need only be an appropriate unit; it need not be the most appropriate unit. See *PCC Structurals, Inc.*, 365 NLRB No. 160, slip op. at 12 (2017)." *Audio Visual Services Group, LLC*, 370 NLRB No. 39, slip op. at 2 (2020).

For the reasons detailed below, I find that the petitioned-for multi-facility Northern California regional unit is an appropriate unit insofar as it shares a distinct community of interest from employees in the other regions.

1. Skills and Duties

This factor examines whether disputed employees can be distinguished from one another on the basis of skills or duties. If they cannot be distinguished, this factor weighs in favor of including the disputed employees in one unit. Evidence that employees perform the same basic function or have the same duties, that there is a high degree of overlap in job functions or of performing one another's work, or that disputed employees work together as a crew, support a finding of similarity of functions. Evidence that disputed employees have similar requirements to obtain employment; that they have similar job descriptions or licensure requirements; that they participate in the same employer training programs; and/or that they use similar equipment supports a finding of similarity of skills. *Casino Aztar*, 349 NLRB 603 (2007); *J.C. Penny Company*, *Inc*., 328 NLRB 766 (1999); *Brand Precision Services*, 313 NLRB 657 (1994); *Phoenician*, 308 NLRB 826 (1992). Where there is also evidence of similar terms and conditions of employment and some functional integration, evidence of similar skills and functions can lead to a conclusion that disputed employees must be in the same unit, in spite of lack of common supervision or evidence of interchange. *Phoenician*, supra.

In this case the record reveals that employees in the petitioned-for Northern California unit cannot be distinguished from the employees the Employer contends should be included in the unit on the basis skills and duties. Members of the IoMT Cybersecurity Field Team all do exactly the same work in the same way, train on the same software, and can be interchanged if needed. The job description and qualifications are the same. The only difference in skills and duties shown in

the record is that facility accreditation standards with respect to IoMT devices vary by state, but the record does not indicate the extent of the variation. This factor weighs in favor of a nationwide unit as advocated for by the Employer.

2. Terms and Conditions of Employment

Terms and conditions of employment include whether employees receive similar wage ranges and are paid in a similar fashion (for example hourly); whether employees have the same fringe benefits; and whether employees are subject to the same work rules, disciplinary policies and other terms of employment that might be described in an employee handbook. However, the facts that employees share common wage ranges and benefits or are subject to common work rules do not warrant a conclusion that a community of interest exists where employees are separately supervised, do not interchange and/or work in a physically separate area. *Bradley Steel, Inc*., 342 NLRB 215 (2004); *Overnite Transportation Company*, 322 NLRB 347 (1996). Similarly, sharing a common personnel system for hiring, background checks and training, as well as the same package of benefits, does not warrant a conclusion that a community of interest exists where two classifications of employees have little else in common. *American Security Corporation,* 221 NLRB 1145 (1996).

In the instant case, the record reveals that employees nationwide share some common terms and conditions of employment, but have significant differences in wages and hours. Wages are calibrated according to the local market, with the effect that employees are paid differently based on geographic region. The 8 a.m. to 5 p.m. working hours mean that there are times of the day when employees in the different regions are not all at work due to time zone differences. Employees otherwise have the same employee handbook, same benefits, same training, undergo the same background checks, and use the same tools to work. The record is light on details of specific benefits. Because employees have different salaries based on geographic region and all employees in the proposed nationwide unit are not at work at the same time for some portion of the day, this factor weighs slightly against a nationwide unit.

3. Employee Interchange

Interchangeability refers to temporary work assignments or transfers between two groups of employees. Frequent interchange "may suggest blurred departmental lines and a truly fluid work force with roughly comparable skills." *Hilton Hotel Corp*., 287 NLRB 359, 360 (1987). As a result, the Board has held that the frequency of employee interchange is a critical factor in determining whether employees who work in different groups share a community of interest sufficient to justify their inclusion in a single bargaining unit. *Executive Resource Associates*, 301 NLRB 400, 401 (1991), citing *Spring City Knitting Co. v. NLRB*, 647 F.2d 1011, 1015 (9th Cir. 1981). In this case, the record fails to reveal evidence of frequent or fluid employee interchange between the employees in Northern California and those in the nationwide unit sought by the Employer. More specifically, while employees can work on devices in other regions, the record shows this does not happen with regularity. Contrary to the Employer's contention, the evidence shows travel between regions is infrequent. The record reveals that while employees can travel between regions, it rarely happens and, importantly, has not happened since the December 2024 inception of the full-time team at issue here.

Also relevant for consideration with regard to interchangeability is whether there are permanent transfers among employees in the unit sought by a union. However, the existence of permanent transfers is not as important as evidence of temporary interchange. *Hilton Hotel Corp*, supra. In any event, there is no evidence in the record of permanent transfers between the employees in the petitioned-for Northern California unit and the nationwide unit sought by the Employer.

The Board has also considered the amount of work-related contact among employees, including whether they work beside one another. Thus, it is important to compare the amount of contact employees in the unit sought by a union have with one another. See for example, *Casino Aztar*, 349 NLRB 603, 605-606 (2007). There is evidence of work-related contact between the petitioned-for Northern California unit and the nationwide unit sought by the Employer, but little evidence of these employees working side by side on the same tasks. The weekly team meetings appear to be focused on information and delivery, rather than meetings where employees actively perform tasks together. While employees may discuss troubleshooting or common issues, ultimately their assigned tasks are separate. While the record shows that it is possible for employees to volunteer or be told to travel to other regions, it also shows that this has not happened since the company completed hiring its directly-employed IoMT Cybersecurity Field Team in December 2024, and that when prior contractors did travel to facilities, they performed work alone, sometimes on different floors of the same facility. Because the employees all work 8 a.m. to 5 p.m. in their respective time zones, they are not all working at the same time. There is a three-hour time difference between California and the East Coast, and six hours between Hawaii and the East Coast. Thus, the nature of their work, the location of their work determined by time zone and location of medical devices, there is limited ability for contact or temporary interchange. Indeed, there is limited evidence of temporary interchange and no evidence of how often that interchange might occur. Therefore, this factor weighs against a nationwide unit.

4. Functional integration

As explained by the Board, "[f]unctional integration involves employees at the various facilities participating equally and fully at various stages in the employer's operation, such that the employees constitute integral and indispensable parts of a single work process." *AT&T Mobility Services*, 371 NLRB No. 14, slip op. at 12 (August 2, 2021). "Evidence that employees work together on the same matters, have frequent contact with one another, and perform similar functions is relevant when examining whether functional integration exists. *Publix Super Markets, Inc.*, 343 NLRB 1023, 1024-1025 (2004); *Transerv Systems*, 311 NLRB 766 (1993). "The Board has found that the factors of employee interchange and functional integration weigh in favor of a petitioned-for multifacility unit where the petitioned-for employees have substantially more contact and interchange with each other than they do with excluded employees." *Audio Visual Services Group*, 370 NLRB No. 39, slip op. at 2 (citations omitted). *Id*. at 3 (finding high level of integration where "petitioned-for jobsites cover almost 95 percent of their own staffing needs and receive only 0.57 percent of their staffing hours from employees who work at the excluded jobsites."). On the other hand, if functional integration does not result in contact among employees in the unit sought by a union, the existence of functional integration has less weight." *Ikea Distribution Servs., Inc.*, 370 NLRB No. 109, slip op. at 16 (Apr. 19, 2021).

In this matter the record reveals that employees in Northern California and those in the rest of the country can work together on the same matters, but collaboration is not regularly essential. However, they are weekly team meetings for the exchange of information and a nationwide Microsoft Teams chat. Therefore, this factor is neutral.

5. Geographic Proximity

"The Board has found the factor of geographic proximity to favor petitioned-for [multifacility] units." *Audio Visual Services Group*, 370 NLRB No. 39, slip op. at 3 (citations omitted). See also *Cazanove Opici Wine Grp.*, 371 NLRB No. 30, slip op. at 2 (Oct. 8, 2021) (finding that geographic proximity "strongly weigh[ed] in favor" of a petitioned-for multi-unit facility in metro New York because the closest Upstate New York facility was 150 miles away, and the furthest was 300 miles away from New York City); *AT&T Mobility Services*, 371 NLRB No. 14, slip op. at 2 (finding that geographic proximity and the fact that "the petitioned-for locations cover a defined geographic area in which no excluded location is located" support finding proposed unit appropriate); cf. *Laboratory Corp. of America*, 341 NLRB at 1079, 1082 (finding unit inappropriate where employer's "organizational structure [was] based on geography" and petitioned-for facilities did not "constitute a coherent geographic grouping."). The Board has given significant weight to a unit's "geographic coherence" in determining a unit's community of interest, even where the unit does not correspond to any single administrative division of an employer. *Central Power & Light Co.*, 195 NLRB 743, 745–746 (1972); see also *Panera Bread*, 361 NLRB 1236, 1236 fn. 1 (2014); *Drug-Fair Community Drug Co.*, 180 NLRB 525, 527 fn. 10 (1969).

In *Cazanove*, supra, the Board decided that geographical proximity "strongly" weighed in favor of the petitioned-for unit, citing distances of between 150 to 300 miles between the closest and furthest metro New York and Upstate New York regions. In *Audio Visual Services Group*, supra, the Board found that where the excluded closest jobsite to the petitioned-for multifacility unit was over 70 miles away, the factor of geographic proximity weighed in favor of the petitioned-for unit. *Audio Visual Services Group* at 4. "While the Board has found that geographic proximity weighs against petitioned-for units when the distances between petitioned-for and excluded facilities are roughly equivalent to the distances between some of the petitioned-for facilities (thus rendering the exclusions somewhat arbitrary), that is not the case here.". *Id*.

The record shows that the IoMT Cybersecurity Field Team Leads and Specialists have been separated by the Employer into separate departments organized by geographic region where its facilities are located. Northern California is a significantly larger region, operations-wise, than the rest, with 21 hospitals and 209 medical offices. The next highest numbers are 15 hospitals and 197 medical offices in Southern California. Only Hawaii and the Northwest regions have any hospitals, and the rest of the regions all have fewer than 55 medical offices and no hospitals. The Employer has explicitly separated Northern and Southern California, even though they are in the same state. While the record does not specify how many miles apart the Northern California region is from the employer's other geographic regions, public knowledge indicates that all but one of these regions are in different states, and the regions in Hawaii, Colorado, Georgia, Virginia, Maryland,

and Washington, D.C. are in different time zones. This factor weighs heavily in favor of the petitioned-for bargaining unit.

6. Centralized control of management and supervision

Another community-of-interest factor is whether the employees in dispute are subject to centralized control of management and supervision. In examining supervision, most important is the identity of employees' supervisors who have the authority to hire, to fire or to discipline employees (or effectively recommend those actions) or to supervise the day-to-day work of employees, including rating performance, directing and assigning work, scheduling work, and providing guidance on a day-to-day basis. *Executive Resources Associates*, supra at 402; *NCR Corporation*, 236 NLRB 215 (1978). Common supervision weighs in favor of placing the employees in dispute in one unit. However, the fact that two groups are commonly supervised does not mandate that they be included in the same unit, particularly where there is no evidence of interchange, contact or functional integration. *United Operations*, supra at 125. Similarly, the fact that two groups of employees are separately supervised weighs against their inclusion in the same unit. However, separate supervision does not mandate separate units. *Casino Aztar*, supra at 607, fn 11. Rather, more important is the degree of interchange, contact and functional integration. Id. at 607.

Here, Manager of Program Management Bernadette O'Doherty manages the three IoMT Cybersecurity Leads. However, the assignment of specific tasks is delegated to the IoMT Team Leads. These Leads are assigned to teams of Specialists based on the Employer's geographic region as described above. The petitioned-for unit employees are on a separate team with a separate Northern California Lead, Greg Marcisz, who only delegates work to Northern California Specialists. Furthermore, Marcisz was responsible for making hiring requests, managing and conducting interviews, and had the final say in who was hired as Specialist in Northern California. Marcisz is also responsible for reviewing Specialists' requests for sick days or vacation. Lead Rex Andrade performs the equivalent tasks for Southern California Employees, and Lead Andrew Whittier performs those tasks for the Markets Outside California. The record was silent regarding who has the authority to hire, fire, or to discipline employees, to rate their performance, and provide guidance on a day-to-day basis. The Employer's choice to use a regional candidate interviewing and selection process and then organize those employees' work assignment process regionally into Northern California, Southern California, and Markets Outside California weighs in favor of the petitioned-for bargaining unit, but the scant record on the remaining elements renders this factor neutral.

7. Bargaining history

The parties have no bargaining history. This factor is neutral.

8. Conclusion

I have carefully weighed the multifacility community of interest factors cited in *Laboratory Corp. of America Holdings*, supra. *Audio Visual Services Group,* supra*,* and conclude that the unit sought by Petitioner consisting solely of the IoMT Leads, Clinical Systems Engineers – IoMT Specialists, and Biomedical Engineering Chief Engineers at the Employer's Northern California facilities is an appropriate unit.

The strongest factor relative to the others weighed in making this determination is geographic proximity. In *Cazanove Opici Wine Grp.*, 371 NLRB No. 30 (Oct. 8, 2021), the petitioned-for unit consisted of sales representatives assigned to six regions/teams in the metropolitan New York area who both worked from home and "in the field visiting customers", analogous to the petitioned-for unit in the present case. *Id*. at 1. The Employer in *Cazanove* argued that those employees should be in the same unit with their counterparts in its four regions/teams in Upstate New York. *Id*. The Board in *Cazanove* applied the analytical framework used in *Audio Visual Services Group, LLC*, 370 NLRB No. 39 (2020) to decide that the remote employees in the petitioned-for geography-based unit shared a community of interest that was distinct from the statewide unit the Employer sought. *Cazanove* at 1. Here, the Employer has deliberately organized its employees in the IoMT Cybersecurity Field Team into geography-based regions that are much farther apart than those in either of the two controlling cases for this factor.

Moreover, the Employer has organized its workflow along regional lines. The employees either work from home or travel to the facilities within their region, they receive assignments and seek time off approvals from regionally-based Leads, and while the record shows that interchange is possible, there is no evidence of meaningful interchange and functional integration occurring after these particular employees were hired.

Both the centralized control of management and supervision, and the lack of bargaining history between the two parties are neutral factors.

In sum, based on the Employer-designed geographic regions showing the great distance between the petitioned for unit Northern California region and the other regions nationwide, the differences in wages along those regional lines, and lack of meaningful employee interchange and functional integration between regions, establishes that the Northern California region is an appropriate bargaining unit distinct from the other regions.

C. ELECTION MODE

The Union seeks an in-person election and argues that it should be held at one of the Employer's facilities located near the majority of the employees' homes. The Employer desires a mail-ballot election and does not agree to hold an in-person election at its Walnut Creek, California facility.

The Board's longstanding policy is that elections should, as a general rule, be conducted manually. However, a Regional Director may reasonably decide to conduct an election by mail

ballot "where circumstances tend to make it difficult for eligible employees to vote in a manual election" or where a manual election is not practical. See NLRB Casehandling Manual (Part Two) Representation Proceedings, Sec. 11301.2.15. In this regard, the Board has provided further guidance:

> When deciding whether to conduct a mail ballot election…, the Regional Director should take into consideration at least the following situations that normally suggest the propriety of using mail ballots: (1) where eligible voters are "scattered" because of their job duties over a wide geographic area; (2) where eligible voters are "scattered" in the sense that their work schedules vary significantly, so that they are not present at a common location at common times;[FN 7 omitted] and (3) where there is a strike, a lockout or picketing in progress. If any of the foregoing situations exist, the Regional Director, in the exercise of discretion, should also consider the desires of all the parties, the likely ability of voters to read and understand mail ballots, the availability of addresses for employees, and finally, what constitutes the efficient use of Board resources, because efficient and economic use of Board agents is reasonably a concern.

In *San Diego Gas and Electric*, 325 NLRB 1143, 1145 (1998), the Board found that "employees may be deemed to be 'scattered' where they work in different geographic areas, work in the same areas but travel on the road, work different shifts, or work combinations of full-time and part-time schedules." *Id.* at 1145 fn.7.

After careful consideration of the parties' positions, I conclude that the election in this matter should be conducted via the mail ballot procedure. It is undisputed that employees are geographically scattered in the sense that all of the employees in question work from home and there is not a time when they are all at the Employer's facilities at the same time for their work duties.

In sum, the undisputed facts establish that a manual election in this case is likely to disenfranchise employees due to a substantial number of eligible voters being scattered. Accordingly, in order to enfranchise the entire unit and provide them with an opportunity to vote free from the appearance of impropriety, the election will be conducted by mail.

CONCLUSION

Based upon the entire record in this matter and in accordance with the discussion above, I conclude and find as follows:

1. The hearing officer's rulings made at the hearing are free from prejudicial error and are hereby affirmed.

2. The Employer is engaged in commerce within the meaning of the Act, and it will effectuate the purposes of the Act to assert jurisdiction herein.

3. The Petitioner is a labor organization within the meaning of Section 2(5) of the Act and claims to represent certain employees of the Employer.

4. A question affecting commerce exists concerning the representation of certain employees of the Employer within the meaning of Section 9(c)(1) and Section 2(6) and (7) of the Act.

5. The following employees of the Employer constitute a unit appropriate for the purpose of collective bargaining within the meaning of Section 9(b) of the Act:

Included: All full-time and regular part-time IoMT Specialists – Cybersecurity Field Team and IoMT Leads – Cybersecurity Field Team employed by the Employer in its Northern California areas for all Employer facilities and locations in Northern California.

Excluded: All other employees, employees represented by a labor organization, managers, confidential employees, office clerical employees, guards, and supervisors as defined by the Act.

DIRECTION OF ELECTION

The National Labor Relations Board will conduct a secret ballot election among the employees in the unit found appropriate above. Employees will vote whether or not they wish to be represented for purposes of collective bargaining by International Union of Operating Engineers, Stationary Engineers, Local 39, AFL-CIO.

A. Election Details

The election will be conducted by United States mail.

The ballots will be mailed to employees employed in the appropriate collective-bargaining unit. At 5:00 PM on **Friday, August 22, 2025**, ballots will be mailed to voters from the National Labor Relations Board, Region 32, 1301 Clay Street, Suite 1510N, Oakland, CA 94612. Voters must sign the outside of the envelope in which the ballot is returned. Any ballot received in an envelope that is not signed will be automatically void.

Those employees who believe that they are eligible to vote and did not receive a ballot in the mail by **Friday, August 29, 2025,** should communicate immediately with the National Labor Relations Board by either calling the Region 32 Office at **1-510-637-3300** or Nicholas L. Tsiliacos **(510) 671-3046.**

All ballots will be commingled and counted at the Region 32 Office on September 4, 2025, at 3:00 p.m. In order to be valid and counted, the returned ballots must be received in the Region 32 Office prior to the counting of the ballots.

B. Voting Eligibility

Eligible to vote are those in the unit who were employed during the payroll period ending **Saturday, August 2, 2025**, including employees who did not work during that period because they were ill, on vacation, or temporarily laid off. Also eligible to vote are all employees in the unit who have worked an average of four (4) hours or more per week during the 13 weeks immediately preceding the eligibility date for the election. In a mail ballot election, employees are eligible to vote if they are in the unit on both the payroll period ending date and on the date they mail in their ballots to the Board's designated office.

Employees engaged in an economic strike, who have retained their status as strikers and who have not been permanently replaced, are also eligible to vote. In addition, in an economic strike that commenced less than 12 months before the election date, employees engaged in such strike who have retained their status as strikers but who have been permanently replaced, as well as their replacements, are eligible to vote. Unit employees in the military services of the United States may vote if they appear in person at the polls.

Ineligible to vote are (1) employees who have quit or been discharged for cause since the designated payroll period, and, in a mail ballot election, before they mail in their ballots to the Board's designated office; (2) striking employees who have been discharged for cause since the strike began and who have not been rehired or reinstated before the election date; and (3) employees who are engaged in an economic strike that began more than 12 months before the election date and who have been permanently replaced.

C. Voter List

As required by Section 102.67(l) of the Board's Rules and Regulations, the Employer must provide the Regional Director and parties named in this decision a list of the full names (that employees use at work), work locations, shifts, job classifications, and contact information (including home addresses, available personal email addresses, and available home and personal cell telephone numbers) of all eligible voters. The Employer must also include in a separate section of that list the same information for those individuals who, according to this direction of election, will be permitted to vote subject to challenge.

To be timely filed and served, the list must be *received* by the regional director and the parties by August 19, 2025. The list must be accompanied by a certificate of service showing service on all parties. **The region will no longer serve the voter list.**

Unless the Employer certifies that it does not possess the capacity to produce the list in the required form, the list must be provided in a table in a Microsoft Word file (.doc or docx) or a file that is compatible with Microsoft Word (.doc or docx). The first column of the list must begin with each employee's last name and the list must be alphabetized (overall or by department) by last name. Because the list will be used during the election, the font size of the list must be the equivalent of Times New Roman 10 or larger. That font does not need to be used but the font must be that size or larger. A sample, optional form for the list is provided on the NLRB website at www.nlrb.gov/what-we-do/conduct-elections/representation-case-rules-effective-april-14-2015.

When feasible, the list shall be filed electronically with the Region and served electronically on the other parties named in this decision. The list may be electronically filed with the Region by using the E-filing system on the Agency's website at www.nlrb.gov. Once the website is accessed, click on **E-File Documents**, enter the NLRB Case Number, and follow the detailed instructions.

Failure to comply with the above requirements will be grounds for setting aside the election whenever proper and timely objections are filed. However, the Employer may not object to the failure to file or serve the list within the specified time or in the proper format if it is responsible for the failure.

No party shall use the voter list for purposes other than the representation proceeding, Board proceedings arising from it, and related matters.

D. Posting of Notices of Election

Pursuant to Section 102.67(k) of the Board's Rules, the Employer must post copies of the Notice of Election accompanying this Decision in conspicuous places, including all places where notices to employees in the unit found appropriate are customarily posted. The Notice must be posted so all pages of the Notice are simultaneously visible. In addition, if the Employer customarily communicates electronically with some or all of the employees in the unit found appropriate, the Employer must also distribute the Notice of Election electronically to those employees. The Employer must post copies of the Notice at least 3 full working days prior to 12:01 a.m. of the day of the election and copies must remain posted until the end of the election. For purposes of posting, working day means an entire 24-hour period excluding Saturdays, Sundays, and holidays. However, a party shall be estopped from objecting to the nonposting of notices if it is responsible for the nonposting, and likewise shall be estopped from objecting to the nondistribution of notices if it is responsible for the nondistribution. Failure to follow the posting requirements set forth above will be grounds for setting aside the election if proper and timely objections are filed.

RIGHT TO REQUEST REVIEW

Pursuant to Section 102.67 of the Board's Rules and Regulations, a request for review may be filed with the Board at any time following the issuance of this Decision until 10 business days after a final disposition of the proceeding by the Regional Director. Accordingly, a party is not precluded from filing a request for review of this decision after the election on the grounds that it did not file a request for review of this Decision prior to the election. The request for review must conform to the requirements of Section 102.67 of the Board's Rules and Regulations.

A request for review must be E-Filed through the Agency's website and may not be filed by facsimile. To E-File the request for review, go to www.nlrb.gov, select E-File Documents, enter the NLRB Case Number, and follow the detailed instructions. If not E-Filed, the request for review should be addressed to the Executive Secretary, National Labor Relations Board, 1015 Half Street SE, Washington, DC 20570-0001, and must be accompanied by a statement explaining the

circumstances concerning not having access to the Agency's E-Filing system or why filing electronically would impose an undue burden. A party filing a request for review must serve a copy of the request on the other parties and file a copy with the Regional Director. A certificate of service must be filed with the Board together with the request for review. Neither the filing of a request for review nor the Board's granting a request for review will stay the election in this matter unless specifically ordered by the Board.

Dated: August 15, 2025

Christy J. Kwon
Regional Director
National Labor Relations Board
Region 32
1301 Clay St Ste 1510N
Oakland, CA 94612-5224