FEDERAL GOVERNMENT CONTRACTING TERMS FOR SUBCONTRACTORS SCHEDULE
Last Updated: September 24, 2025

Omnicell, Inc. ("**Omnicell**") and Subcontractor (as hereinafter defined) have entered into an agreement ("**Underlying Agreement**") whereby Omnicell purchases goods or services from Subcontractor where such goods and/or services will be resold to the U.S. Government. Omnicell has an agreement with the federal government ("**Prime Agreement**"). This Federal Government Contracting Terms for Subcontractors Schedule ("**Government Contracting Schedule**") sets forth the obligations of Subcontractor with respect to Omnicell's US Government customers. In cases of conflict between this Government Contracting Schedule and the Underlying Agreement, this Government Contracting Schedule will prevail. As used in this Government Contracting Schedule, "**Subcontractor**" means the entity or individual (whether a manufacturer, distributor, vendor, or other supplier) and its respective employees, personnel, and agents that is providing goods, services, and/or products to Omnicell pursuant to the Underlying Agreement for resale to the U.S. Government under the Prime Agreement.

In the U.S. Government clauses contained in this Government Contracting Schedule, unless the context of the clause requires otherwise, the term "**Contractor**" shall mean Subcontractor, the term "**Contract**" shall mean the Underlying Agreement including this Government Contracting Schedule, and the terms "**Government**," "**Contracting Officer**" and equivalent phrases shall mean Omnicell and Omnicell's Contractual Representative, respectively. It is intended that these clauses shall apply to Subcontractor in such manner as is necessary to reflect the position of Subcontractor as a subcontractor to Omnicell, to ensure the Subcontractor's obligations to Omnicell and to the United States Government, and to enable Omnicell and Subcontractor to meet their obligations under Omnicell's Prime Agreement and the Underlying Agreement. Unless otherwise stated, all definitions defined by FAR 2.101 shall be applied to the terms referenced herein.

To the extent that the Prime Agreement is modified (to include a newer version of any such clause), the date of the modified version of the clause as it appears in such Prime Agreement shall be controlling and said version shall be incorporated herein.

PART A: FLOW DOWN CLAUSES

The full text of the clauses incorporated by reference below can be found at: FAR | Acquisition.GOVA.1. Subcontractor agrees to adhere to those clauses set forth in the Prime Agreement or applicable to the Prime Agreement, all of which are incorporated by reference and made a part of this Government Contracting Schedule, including the following:

FAR 52.203-6 Restrictions on Subcontractor Sales to the Government (June 2020) Alt. I

FAR 52.203-13 Contractor Code of Business Ethics and Conduct (NOV 2023)

FAR 52.203-17 Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights (APR 2014)

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

FAR 52.203-19 Contractor Employee Whistleblower Rights (NOV 2023)

FAR 52.204-10 Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020)

FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2021)

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEC 2023)

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (NOV 2021)

FAR 52.204-27 Prohibition on a ByteDance Covered Application (JUN 2023)

FAR 52.204-30 Federal Acquisition Supply Chain Security Act Orders—Prohibition (DEC 2023)

FAR 52.219-8 Utilization of Small Business Concerns

FAR 52.222-19 Child Labor – Cooperation with Authorities and Remedies (JAN 2025)

FAR 52.222.21 Prohibition of Segregated Facilities

FAR 52.222.26 Equal Opportunity

FAR 52.222-35 Equal Opportunity for Veterans (JUN 2020)

FAR 52.222-36 Equal Opportunity for Workers with Disabilities (JUN 2020)

FAR 52.222-37 Employment Reports on Veterans (JUN 2020)

FAR 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (DEC 2010)

FAR 52.222-50 Combating Trafficking in Persons (NOV 2021)

FAR 52.223-11 Ozone-depleting Substances and High Global Warming Potential Hydrofluorocarbons (MAY 2024)

FAR 52.223-20 Aerosols (MAY 2024)

FAR 52.223-21 Foams (MAY 2024)

FAR 52.225-13 Restrictions on Certain Foreign Purchases (FEB 2021)

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

FAR 52.226-8 Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024)

FAR 52.227-14 Rights in Data-General (May 2014) (ALTERNATE III – DEC 2007)

FAR 52.246-2 Inspection of Supplies – Fixed Price (AUG 1996)

VAAR 852.212-71 Gray Market and Counterfeit Items (FEB 2023)

FAR 52.224-3 Privacy Training (JAN 2017)

FAR 52.225-5 Trade Agreements (NOV 2023)

FAR 52.225-6 Trade Agreements Certificate (FEB 2021)

To the extent Subcontractor is providing hardware or software that will be resold to the U.S. Government, SUBCONTRACTOR will complete the following Certificate and return to Omnicell.

(a) The contractor certifies that each end product, except those listed in paragraph (b) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this Schedule entitled "Trade Agreements."

(b) The contractor shall list as other end products those supplies that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin

[*List as necessary*]

(c) [Reserved]

(End of clause)

VAAR 852.204-71 Information and Information Systems Security (FEB 2023)

PART B: SPECIAL TERMS AND CONDITIONS

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

To the extent Subcontractor is providing services to U.S Government customers in Veterans Affairs, Subcontractor agrees to adhere to the requirements set forth in this Section B.

B.1. Department of Veterans Affairs Information and Information System Security and Privacy Requirements

B.1.1. VA Information Custodial Language

B.1.1.a. Information made available to the Subcontractor by the Department of Veterans Affairs or by Omnicell (as used in Section B to the Government Contracting Schedule, "VA") for the performance or administration of the Underlying Agreement will be used only for the purposes specified in the Subcontract. The Subcontractor shall not use VA information in any other manner without prior written approval from Omnicell.

B.1.1.b. VA information will not be co-mingled with any other data on the Subcontractor's information systems or media storage systems. The Subcontractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

B.1.1.c. Omnicell reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Subcontractor Information Technology ("IT") resources to ensure information security is compliant with Federal and VA requirements. The Subcontractor shall provide all necessary access to records (including electronic and document materials related to this Subcontract) and support (including access to Subcontractor staff associated with this Subcontract) to Omnicell during periodic control assessments, audits, or investigations arising out of the performance of this Subcontract.

B.1.1.d. The Subcontractor may only use VA information within the terms of this Subcontract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations, or VA policies become applicable after execution of the contract, the parties agree to negotiate modification of this Subcontract and adjustment necessary to implement the new laws, regulations, and/or policies.

B.1.1.e. The Subcontractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of this Subcontract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

B.1.1.f. The Subcontractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at minimum, Federal Information Processing Standards ("FIPS") 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service Requirements. The Subcontractor shall transmit VA sensitive information using VA approved Transport Layer Security ("TLS") configured with FIPS based cipher suites in conformance with National Institute of

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

Standards and Technology (“NIST”) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

B.1.1.g. The Subcontractor’s firewall and web services security controls, as applicable, shall meet or exceed the VA’s minimum requirements.

B.1.1.h. Except for uses and disclosures of VA information authorized by this Subcontract for performance of this Subcontract, the Subcontractor may use and disclose VA information only (i) in response to a qualifying order of a court of competent jurisdiction after notification to the VA Contracting Officer and to Omnicell and (ii) with written approval from the VA Contracting Officer. The Subcontractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to Omnicell.

B.1.1.g. Notwithstanding the provision above, the Subcontractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality-assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (“HIV”). If the Subcontractor is in receipt of a court order or other requests for the above-mentioned information, the Subcontractor shall immediately refer such court order or other requests to Omnicell.

B.1.1.h. Information made available to the Subcontractor by the VA for the performance or administration of this Subcontract or information developed by the Subcontractor in performance or administration of this Subcontract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (“IAM”) Security processes specified in the VA Information Security Knowledge Service.

B.1.1.i. Any data destruction done on behalf of Omnicell by the Subcontractor shall be done in accordance with the National Archives and Records Administration (“NARA”) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

B.1.1.j. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that are used to store, process, or access VA information that cannot be destroyed shall be returned to Omnicell. The Subcontractor shall hold the appropriate material until otherwise directed by Omnicell. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Subcontractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide Omnicell with the tracking information.

B.1.2. Access to VA Information and VA Information Systems

B.1.2.a. The Subcontractor shall sign the VA Information Security Rule of Behavior before commencing access to VA information and information systems. Users who require privileged

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell’s express written consent is prohibited.

access shall complete the VA elevated privilege access request processes before privileged access is granted.

B.1.2.b. The Subcontractor shall notify Omnicell in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes with respect to any person who requires access to information made available to the Subcontractor by the VA for the performance or administration of this Subcontract or information developed by the Subcontractor in performance or administration of this Subcontract. Causes may include the following:

B.1.2.b.1. Subcontractor personnel no longer has a need for access to VA information or VA information systems.

B.1.2.b.2. Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

B.1.2.b.3. Subcontractor believes their own personnel may pose a threat to Omnicell's or the Subcontractor's working environment or to any Omnicell- or Subcontractor-owned property. This includes Omnicell- or Subcontractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

B.1.2.b.4. Any previously undisclosed changes to Subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

B.1.2.b.5. Subcontractor personnel have their authorization to work in the United States revoked.

B.1.2.c. When the Subcontractor no longer requires VA access, the Subcontractor shall return VA-issued property to the VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office.

B.1.3. Training

B.1.3.a. Subcontractor personnel requiring access to VA information and VA information Systems shall successfully complete the following before being granted access to VA information and its systems:

B.1.3.a.1. VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.

B.1.3.a.2. Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

B.1.3.a.3. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access.

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

B.1.3.b. The Subcontractor shall provide to Omnicell a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of this Subcontract and annually thereafter, as required.

B.1.3.c. The Subcontractor is advised that failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on this Subcontract until such time as the required training is complete.

B.1.4. Security Incident Investigation

B.1.4.a. The Subcontractor, its employees, or its business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA Office of Information Technology's Enterprise Service Desk ("ESD") by calling (855) 673-4357 (TTY:711). After reporting to the ESD, the Subcontractor, its employees, or its business associates shall, within one hour, provide the VA and Omnicell the incident number received from the ESD.

B.1.4.b. To the extent known by the Subcontractor, the Subcontractor's notice to the VA and Omnicell shall identify the information involved and the circumstances surrounding the incident, including the following:

B.1.4.b.1. The date and time (or approximation of) the Security Incident occurred.

B.1.4.b.2. The names of individuals involved (when applicable).

B.1.4.b.3. The physical and logical (if applicable) location of the incident.

B.1.4.b.4. Why the Security Incident took place (i.e., catalyst for the failure).

B.1.4.b.5. The amount of data belonging to VA believed to have been compromised.

B.1.4.b.6. The remediation measures the Subcontractor is taking to ensure no future incidents of a similar nature.

B.1.4.c. After the Subcontractor has provided the initial detailed incident summary to the VA and Omnicell, the Subcontractor will continue to provide written updates on any new and relevant circumstances or facts it discovers. The Subcontractor and its employees shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA.

B.1.4.d. In instances of theft or break-in-or other criminal activity, the Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA Office of Inspector General, and the VA Office of Security and Law Enforcement. The Subcontractor and its employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Subcontractor shall cooperate with the VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B.1.4.e. The Subcontractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

B.1.4.f. With respect to unsecured Protected Health Information ("PHI"), the Subcontractor is deemed to have discovered a data breach when the Subcontractor knew or should have known of breach of such information.

B.1.4.g. If the Subcontractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the Subcontractor processes or maintains under this Subcontract, the Subcontractor shall indemnify Omnicell for all liquidated damages required to be paid to the VA by Omnicell attributable to the Subcontractor's failure or conduct pursuant to VAAR 852.211-76, Liquidated Damages – Reimbursement for Data Breach Costs (FEB 2023), including its alternates.

B.1.5. Data Center Provisions

B.1.5.a. The Subcontractor shall ensure the VA network is accessed in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

B.1.5.b. The Subcontractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

B.1.5.c. The Subcontractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces, utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

B.1.5.d. The Subcontractor shall encrypt all traffic across the segment of the Wide Area Network ("WAN") it manages and no unencrypted Out of Band ("OUB") Internet Protocol ("IP") traffic will traverse the network.

B.1.5.e. The Subcontractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

B.1.5.f. The Subcontractor shall secure access from Local Area Networks ("LANs") at co-located sites in accordance with VA TIC References Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information and Security Knowledge Service.

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.

B.2. Federal Government Contracting Requirements. As used in this Subpart, the terms the "Government," the "United States," the "Agency," and similar, shall mean the United States or any Department or Agency thereof, including the Department of Veterans Affairs. The "Company" shall mean Omnicell, Inc.

B.2.1. Services Limited. The Subcontractor shall provide services with respect to products manufactured or sold by Omnicell to the Government or other customers on an as-requested basis ONLY.

B.2.1.1. The Subcontractor shall not provide services with respect to products manufactured or sold by Omnicell except (i) at the direction of Omnicell or (ii) under the supervision of Omnicell and with Omnicell's written consent.

B.2.1.2. The Subcontractor shall only use personnel to provide services to products manufactured or sold by Omnicell who have completed training required by Omnicell before performing such services, including VA Information and Information Systems Security-required training.

B.2.2. Distribution Limited. To the extent the Underlying Agreement is a Distribution Agreement and except as expressly authorized by this Distribution Agreement, and notwithstanding general provisions of this Distribution Agreement to the contrary, the scope of distribution or resale under this Distribution Agreement shall not be construed to permit distribution or resale of products manufactured or sold by Omnicell to the Government by the Distributor.

PART C: AWARD SPECIFIC TERMS AND CONDITIONS

To the extent an award by the U.S. Government to Omnicell contains additional award specific terms, Omnicell will issue an amendment to the Government Contracting Schedule to incorporate the award specific terms and will make those award specific terms available to Subcontractor.

This document contains the Confidential Information of Omnicell, Inc.
Use or disclosure of this document without Omnicell's express written consent is prohibited.