Subordinate User Terms and Conditions for Access to the DLA Internet Bid Board (DIBBS) – effective July 1, 2026

Purpose:

DIBBS allows users to view and quote on DLA solicitations. Through this system, DLA annually awards tens of thousands of simplified acquisition awards, enabling DLA under FAR 13.002 to:

(a) Reduce administrative costs;

(b) Improve opportunities for small, small disadvantaged, women-owned, veteran-owned, HUBZone, and service-disabled veteran-owned small business concerns to obtain a fair proportion of Government contracts;

(c) Promote efficiency and economy in contracting; and

(d) Avoid unnecessary burdens for agencies and contractors.

By accepting these terms and conditions, you are stating and agreeing to the following:

- I am **John Smith**.

- I am an authorized representative for the Commercial and Government Entity Code (CAGE) **DIBBS** and have the authority to use this account for CAGE **DIBBS**.

- I can be reached at phone number **(614) 693-XXXX** and e-mail address **John.Smith@company.com**

- I will use this account for the sole purpose of conducting business with the Defense Logistics Agency (DLA) for CAGE **DIBBS**.

- I have read this entire document and accept as the authorized representative and on behalf of the contractor, the terms and conditions contained herein.

Account Management:

As a DIBBS User for CAGE **DIBBS**:

1. I will notify my company's DIBBS Super User or the DIBBS help desk at dibbsbsm@dla.mil immediately, but in any case, no later than 2 business days when this user account is no longer required.

2. I am a single authorized individual and my account and password shall only be shared with my company's Super User, and not to anyone else, including other employee(s) of the company, agency representatives, and/or third-party services bidding on our company's behalf. My user account will be in my legal name, as reflected on my Government-issued identification (e.g., driver's

license, passport, etc.).

3. I agree that using another individual's email address and password to access DIBBS is strictly prohibited.

4. I will ensure that my account shall have a unique password and a valid email address and telephone number.

5. I agree the address for this company, as registered in the U.S. Government System for Award Management, must meet the requirements of Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance and Information (PGI) 204.1870-2 – Maintenance of the Commercial and Government Entity (CAGE) file. These requirements include that a company's address is the physical address, not a mailbox address, virtual office, or a personal address (unless the physical address of this company is the same as the personal address of the user). Prohibited virtual office addresses include those with a short-term virtual location, such as mobile offices, commercial packaging/mailing facilities (e.g., UPS stores, FedEx stores), mailbox rentals, and certain business incubator locations if the majority of the operations are not performed from that incubator location.

6. I agree that no user account will use any means to mask their internet usage/access to DIBBS or interfere with DLA's ability to identify, authenticate, and geolocate users. This includes, but is not limited to, the use of Virtual Private Networks (VPNs), other proxies, and hosting services (for example, AWS, Google Cloud, Azure).

7. I agree that DLA may restrict my account at any time and require the Super User to obtain additional information before returning my account to full privileges.

8. If the address of this company, as registered in the U.S. Government System for Award Management, is a U.S. address, I agree that I will not access DIBBS outside the United States or U.S. territories without prior approval from DLA.

9. If the address of this company, as registered in the U.S. Government System for Award Management, is an address outside of the U.S., I agree that I will not access DIBBS outside of the country in which I am registered without prior approval from DLA.

Account Access:

Due to the volume of solicitations and awards issued, when access is granted to use DIBBS, DLA relies on all DIBBS users to input accurate information and abide by these terms and conditions as well as those of other DLA systems. The security of the United States Department of Defense, and thus of the United States, depends upon the integrity of the DLA systems, the proper access to the DLA systems, the proper use of data within the DLA system, and the efficiency and ease to validate

information suppliers supply in DLA systems to properly access and use these systems. Consequently, to ensure the integrity of the DLA systems, access to DIBBS may be temporarily denied or indefinitely suspended for any of the following or other appropriate reasons:

- Reasonable suspicion that a supplier's account has been compromised or is being used to adversely impact the automated procurement system.
- Sharing account information with unregistered and/or unauthorized users.
- Any violation of these terms and conditions.
- Use of data, accessed through DLA systems, in violation of the Export Administration Regulations (EAR) and/or International Traffic in Arms Regulations (ITAR).
- Material misrepresentation made in DIBBS.
- A supplier fails to comply with the requirements, when applicable, regarding controlled unclassified information, controlled technical information and covered defense information as set forth in DFARS clauses 252.204-7008, 252.204-7009, 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021.
- A supplier fails to provide required documentation requested by a contracting officer necessary to validate contractor information submitted in DIBBS pursuant to FAR 52.246-2, Procurement Note C03. This includes failure to respond to requests for pre or post award traceability.
- A supplier fails to comply with the provision of FAR clauses 52.204-24 and 52.204-25.
- A supplier quoting a source of supply that does not have DLA controlling authority approval to access export-controlled technical data subject to the exceptions set forth in DLAD PGI 25.7902-4(S-90).
- An individual or supplier is suspended, proposed for debarment, debarred, or voluntarily excluded (FAR 9.405).

DLA will promptly provide notice as to why a DIBBS account is suspended and supply guidance on the reinstatement process by email. Any suspended account will remain suspended until the DIBBS Super User provides sufficient information to demonstrate the account has fully addressed the reason for the suspension and implemented corrective action that mitigates any harm caused to the Government, if necessary. Reinstatement of your DIBBS account does not absolve any misconduct or in any way prohibit DLA from taking action against you and/or your company, including but not limited to criminal, civil, and/or administrative remedies. This also extends to any business entity organized following the suspension of a company's DIBBS account that has the same or similar management, ownership, or principal employees as the suspended contractor or individual.

Additionally, and without advance notice, DLA reserves the right to limit the number of quotations a supplier can submit in DIBBS in a 24-hour period through individual or batch submissions. To ensure the integrity of the DLA systems and supply chains, this right may be taken on individual accounts or for the entire system. Reasons may include cyber-attacks, security concerns, sudden increase in the number of quotes submitted, new user accounts, accounts with an excessive number of contractor-caused cancelations or delinquencies, and for any other reason that may compromise DLA's data systems, or the supply chains supported through DIBBS.

DIBBS and DLA Technical Data Management Transformation (TDMT) are separate programs but are connected. Therefore, if your company is temporarily denied or indefinitely suspended for violating the above terms and conditions, you will be subject to the same denial or suspension from TDMT.

Warning: Unless the conditions for an exception set forth in DLA Acquisition Directive (DLAD) Procedures Guidance and Information (PGI) 25.7902-4(S-90) are met, quoting a source of supply that does not have DLA controlling authority approval to access export-controlled technical data may result in DLA withholding access to DLA-managed export-controlled technical. The DLAD can be found at https://www.dla.mil/Acqusition.

Acknowledgment and Consent:

You also acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

You are accessing a U.S Government Information Systems (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only. You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system. Communications using this information system, or data stored on this information system, are not private and are subject to routine monitoring, intercepting, and searching, and may be disclosed or used for any U.S. Government-authorized purpose.

The U.S. Government may conduct periodic reviews to ensure registrants are abiding by the requirements set forth in PGI 204.1870-2 – Maintenance of the Commercial and Government Entity (CAGE) file.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. government interest-not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications of data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work products are private and confidential, as further explained below:

Nothing in these terms and conditions shall be interpreted to limit a user’s consent to or in any other way restrict or affect any U.S. Government actions for purposes of

network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.