Defense Industrial Base Vulnerability Disclosure Program
Acknowledgement and Agreement to Terms of Service ("Service Agreement")

Subject to the acknowledgments and conditions set forth below, the eligible DoD or other contractor or subcontractor ("Participant") agrees to participate in the Defense Industrial Base Vulnerability Disclosure Program ("DIB-VDP") a crowd-sourced cybersecurity vulnerability reporting and remediation tracking service collaboratively provided by DoD Cyber Crime Center (DC3) ("Sponsor"). DIB-VDP is operationally executed by DC3 within its DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE) and DoD Vulnerability Disclosure Program (VDP) lines of effort.

1. **The Participant understands, acknowledges and accepts that:**

   a) That DIB-VDP is independent of other programs operated or managed by DC3 or DCSA and that the Participant and Sponsor (hereinafter "Parties") obligations regarding DIB-VDP are solely subject to the terms of this Service Agreement;

   b) The Participant will decide, at its sole discretion, which information systems ("Assets") to identify and provide to DIB-VDP to publish to crowd-sourced third-party researchers ("Researchers") for vulnerability testing;

   c) The Researchers are not certified or otherwise affiliated with the U.S. Government in the performance of their cybersecurity research subject to the DIB-VDP policy;

   d) All Assets that the Participant provides to DIB-VDP to publish must be covered contractor information systems, as defined per DFARS 252.204-7012(a), and must be owned or operated by or on behalf of the Participant, and if operated on behalf of the of the Participant by a service provider in a cloud environment, the Assets must be distinguishable so as to be segregated from other portions of the network environment that are outside the scope of vulnerability research;

   e) If Sponsor resources are not sufficient for all eligible applicants to participate, enrollment priority in DIB-VDP will be assigned based on criteria established and applied by the Sponsor which may include: 1) the subject matter of controlled unclassified information within the covered network(s); 2) the size of Participant's relevant contracting activity or covered networks; and 3) earlier execution of the Service Agreement relative to other applicants;

   f) DIB-VDP analysts may perform vulnerability testing to gather additional data to verify the vulnerability, or to test that mitigation is complete;

   g) A Participant will be considered to have mitigated an Asset vulnerability reported under DIB-VDP by either having eliminated it (such as through reconfiguration, software

updates or patching, etc.), or by providing acknowledgment and satisfactory explanation that covered data has been removed so that the Asset is no longer a covered contractor information system;

h) A Participant's report of having mitigated a vulnerability will be validated by DIB-VDP analysts and that DIB-VDP has sole discretion to determine whether a vulnerability has been satisfactorily mitigated;

i) Neither the Participant's voluntary participation in DIB-VDP, nor the reported results of such participation are intended to create any unfair competitive advantage or disadvantage in U.S. Government source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a U.S. Government endorsement or approval of the Participant, its information systems, or its products or services;

j) The Participant's participation or non-participation in DIB-VDP will not, by itself, affect the Participant's National Industrial Security Program facility clearance, if applicable, or the Participant's Cybersecurity Maturity Model Certification (CMMC) or similar rating, if such is established by the DoD, however, Participant may, at its sole discretion, offer its participation in DIB-VDP as evidence of cybersecurity compliance, efficacy or maturity;

k) A reported vulnerability under DIB-VDP is not, in and of itself, considered to be a cyber incident and does not require a mandatory report pursuant to DFARS 252.204-7012(c). However, the Participant's review and efforts to remediate a reported vulnerability may lead to the Participant discovering reportable cyber incidents which may trigger a contractual or other mandatory reporting requirement;

l) The Parties will conduct their respective activities under the Service Agreement, including all amendments, in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data;

m) In accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use and disclosure of electronic communications or data and the voluntary, collaborative nature of the activity described in this Service Agreement, the Parties each bear responsibility for its own actions under DIB-VDP;

n) This Service Agreement does not abrogate the Parties' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or contractual obligation. Participation in DIB-VDP does not eliminate the requirement for a

Participant to report cyber incidents in accordance with legal, regulatory, contractual or other requirements;

o) Data gathered by Researchers and by DIB-VDP personnel will be stored at the unclassified level;

p) All data will be gathered by Researchers and submitted directly to a web portal operated by a third-party contractor, subject to the non-disclosure provisions as contained in this Service Agreement, contracted by Government as an intermediary for crowd-sourced vulnerability reporting. Using a secure connection, Sponsor will obtain this information directly from the third-party contractor and this information will then be disseminated only to the affected Participant through a tailored module within the DoD-owned and operated "Vulnerability Report Management Network" (VRMN);

q) Information shared by the Participant or discovered by Researchers under this program may include sensitive proprietary, commercial, or operational information that is not customarily externally shared, and that the unauthorized use or disclosure of such information might cause substantial competitive harm to the Participant, and that regarding such information:

   i) DIB-VDP will take reasonable steps to protect against the unauthorized use or release of contractor attributional/proprietary information obtained based on participation, and

   ii) DIB-VDP will structure its internal use and disclosure of contractor attributional/proprietary information to disclose only to Sponsor personnel and support contractors, with a reasonable need-to-know, and that are bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information and are engaged in lawfully authorized activities, and

   iii) Participant attributional/proprietary information is maintained within Sponsor to the maximum extent practicable, however, based on a Sponsor determination of a national security purpose or as otherwise required by law, Sponsor may share contractor attributional/proprietary information outside of Sponsor on a need-to-know basis to support authorized Sponsor activities;

r) Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 C.F.R. Parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Sponsor will protect sensitive nonpublic information under DIB-VDP against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or

submitter (e.g., Participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies;

s) Information relating to the vulnerability discovered on the Participant's asset will be stored in a DoD database including, but not limited to: logs, IP addresses, affected domain/application, screenshots, detailed steps of how to replicate the vulnerability, report of expected impact, information identifying the Participant that owns the asset, name and contact information of the Participant's point of contact, name or alias and contact information of reporter, mitigation actions performed by the Participant on the reported asset, follow on items as determined between DIB-VDP and the Participant;

t) Data will be disposed of as per DoD and AF policy (DCIO-01);

u) Other than to publish the Assets identified by the Participant to Researchers, DIB-VDP will not publicize Participant's involvement in DIB-VDP without Participant's consent;

v) That Sponsor may change the terms and conditions of participation in DIB-VDP, prior to which the Participant will have to opportunity to acknowledge and agree according to an updated Service Agreement or to withdraw from DIB-VDP;

w) That Sponsor may share non-attributional/non-proprietary information that was provided by the Participant (or derived from information provided by the Participant) for any lawful purpose;

x) That none of the restrictions on the Sponsor's use or sharing of information in this Service Agreement shall limit the Government's ability to conduct law enforcement or counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements. The results of the activities described in this Service Agreement may be used to support an investigation and prosecution of any individual or organization including those attempting to infiltrate and compromise information on the company's information system in violation of any statute including, but not limited to Title 18, U.S.C., Chapter 37, Espionage and Censorship; the Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2703 et seq.; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Economic Espionage Act, 18 U.S.C. § 1831 et seq.; or like statutes with counterintelligence purposes;

y) That information provided by DIB-VDP to the Participants under this Service Agreement is provided without any guarantee or assurance of its accuracy or effectiveness, and the U.S. Government assumes no liability for Participants' use of or reliance on information disclosed under this Service Agreement; and

z) That the Parties agree to hold the each other harmless regarding any liability arising from information provided in good faith by one Party to the other Party pursuant to this Service Agreement.

2. **The Participant agrees to:**

a) Permit Researchers to test their published resources or assets for vulnerabilities as consistent with the DIB-VDP policy;

b) Using the standardized request and certification process, provide DIB-VDP with, and maintain up-to-date, IP addresses, URLs, hosts or other information to be published to Researchers that satisfactorily identify the Participant's eligible Assets that are within the scope of vulnerability research;

c) Act reasonably and in good faith in mitigating reported vulnerabilities according to a timeline provided by DIB-VDP based on the classification of the severity of the vulnerability, and to maintain contact with DIB-VDP, and, as necessary, the Researcher, until the vulnerability has been successfully mitigated; and

Note: To ensure efficient use of DIB-VDP resources, a Participant's failure to mitigate a reported vulnerability within the acceptable timeframe after reasonable consultation may result, at the sole discretion of Sponsor, in the Participant being removed from DIB-VDP.

d) Provide a points of contact for DIB-VDP to communicate with regarding:

Program participation or consent;
Vulnerability reports and associated information; and
Mitigating reported vulnerabilities;

e) Not to pursue action, whether criminal or civil, against a Researcher, who, after Participant has consulted with DIB-VDP, has been determined by DIB-VDP to have acted in good faith and in compliance with the DIB-VDP policy. Such obligation will extend beyond Participant's withdrawal from DIB-VDP and removal of publication or IP addresses or similar information regarding Researchers who have acted in good faith based on prior published information.

3. **Expiration or Termination of the Service Agreement:**

a) The Service Agreement will remain in force until expiration or termination. If not earlier terminated, the Service Agreement expires three years from the date of Participant signature. The Participant may reapply for participation in DIB-VDP, as available;

b) The Participant may discontinue participation in DIB-VDP at any time, by providing the Sponsor with written notice of the termination of this Service Agreement;

c) At Sponsor discretion or based on violation of the terms this Service Agreement, Participant's participation in DIB-VDP may be terminated.

d) Upon expiration or termination of the Service Agreement, the Sponsor will cooperate to cease any DIB-VDP activities herein as soon as reasonably practicable and, in any event, no later than 10 business days after the date of expiration or termination. Additionally, the Participant's scope and asset information may be maintained for a reasonable period of time to support review of Researcher activity regarding compliance with DIB-VDP Policy; and

e) Termination is the sole remedy for violation of the terms of this Service Agreement; however, the rights and remedies of the parties that arise from any other source are not affected.

4. **Express Statement pursuant to Critical Infrastructure Information Act of 2002:**

As represented by the signatory, any information that Participant provides to DIB-VDP pursuant to its participation is voluntarily submitted to the federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002, as amended by the Cybersecurity and Infrastructure Security Act of 2018.

5 . **Signature and Points of Contact:**

Company Name	Address / City / State / Zip	
Primary POC: Name / Role	Signature	Date
Secondary POC: Name / Role	Signature	Date