Fortreum, LLC
44679 Endicott Drive
Suite 328
Ashburn, VA 20147
Tel 1-703-957-0204
www.fortreum.com

July 25, 2022

GitLab Inc.
268 Bush Street #350
San Francisco, CA 94104

To whom it may concern,

At the request of GitLab, Inc., Fortreum, LLC (Fortreum), an accredited Third-Party Assessment Organization (3PAO) conducted an assessment of the GitLab application to validate the implementation of the cryptographic security functions in accordance with Federal Information Process Standards (FIPS) 140-2. The purpose of the assessment was to validate that all approved security functions within the GitLab application were configured to be conformant with all FIPS 140-2 requirements for transmissions, symmetric key functions and decryption, digital signature, message authentication, and hashing. Additionally, Forteum validated that the GitLab application leverages the following FIPS 140-2 validated cryptographic modules:

- Ubuntu 20.04 AWS Kernel Crypto API Cryptographic Module (#4132)
- Ubuntu 20.04 OpenSSL Cryptographic Module (#3966)
- Ubuntu 20.04 Libgcrypt Cryptographic Module (#3902)
- Amazon Linux 2 Kernel Crypto API Cryptographic Module (#3709)
- Amazon Linux 2 OpenSSL Cryptographic Module (#3553)
- RedHat Enterprise Linux 8 OpenSSL Cryptographic Module (#4271)
- RedHat Enterprise Linux 8 Libgcrypt Cryptographic Module (#3784)

GitLab is a DevOps software that combines the ability to develop, secure, and operate software in a single application. GitLab is an open-source project with over 3,000 contributors that spans the entire software development lifecycle. The GitLab application is comprised of the following technology components: Ingress Controller, NGINX, gitlab-shell, Pages, Workhorse, Rails, Runner, Gitaly, Redis, Container Registry, and PostgreSQL. These components are the default technology base, but customers also have the ability to configure GitLab to integrate with additional components.

During the period of May 2, 2022, through July 25, 2022, Fortreum, LLC. performed an assessment of the GitLab application to validate the implementation of the FIPS-approved security functions in accordance with FIPS 140-2. The methodology used to conduct the security assessment of the GitLab application was based upon the Risk Management Framework outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations. The GitLab application assessment was performed in accordance with NIST SP-800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. The following version was used for testing:

- Omnibus GitLab:
  - Package: gitlab-fips
  - Version: 15.2.0-fips
- Cloud Native GitLab (Helm Chart)

- Version: 6.2.0

The GitLab application is known to operate on the following operating systems:

- Omnibus GitLab: Ubuntu 20.04 LTS
- Cloud Native GitLab: Amazon Linux 2 (EKS)

During the assessment of the GitLab web application, assessors identified a total of zero gaps based on the validation of GitLab's cryptographic implementation for each application component.

Fortreum, LLC. attests that the GitLab assessment testing provides a complete assessment of the applied cryptographic algorithms. Evidence to validate the successful implementation of the various security controls has been collected and validated.

A copy of this letter with all supporting security assessment documentation should be retained in accordance with the Organization's record retention schedule. If you have any questions about the design review the Fortreum team performed, please contact info@fortreum.com.

Sincerely,

Michael Carter

Fortreum, LLC
44679 Endicott Drive, Suite 328 Ashburn, VA 20147
info@fortreum.com
+1 703-957-0204