SERA BRYNN®
CYBER RISK MANAGEMENT

June 11, 2021

Princeton University
Research Computing
Princeton, New Jersey

Subject: – Princeton University Citadel Compliance with CMMC Level 3

Introduction
The purpose of this letter is to describe the Cybersecurity Maturity Model Certification (CMMC) Maturity Level (ML) 3 requirements being met by the Princeton University Citadel system. Obtaining a CMMC ML3 certification requires the Princeton University Citadel system to fully implement all requirements.

Findings
Sera-Brynn, a cyber risk management audit and advisory firm, is an independent Third-Party Assessment Organization (3PAO) under the Federal Risk and Authorization Management Program (FedRAMP) program, conducted an independent assessment of the Princeton University Citadel system. Our findings indicate:

- As of June 11, Princeton University Citadel has fully implemented 90%.
- All partially implemented or planned requirements have an appropriate plan of action to remediate any deficiencies.
- The technical configuration of the system poses a **low** risk to any controlled unclassified information (CUI) stored within the system.

For the Department of Defense (DoD), CMMC will increase the number of requirements necessary to allow CUI to be processed within a non-federal system. However, at the time of this assessment, the CMMC program was still undergoing testing and is not final. Continuing to work towards addressing the controls not fully implemented, Princeton University Citadel system should be appropriately postured to obtain a CMMC ML 3 certification.

If you have any questions concerning this effort, please contact me at (773) 302-1330 or alexy.johnson@sera-brynn.com.

Sincerely,

Alexy Johnson
Director of Compliance