85 Devonshire Street, 8th Floor | Boston, MA 02109 | (857) 957-0345

PreVeil Statement on DFARS 7012
Dated: March 31, 2021

PreVeil Inc. accepts the requirements of *DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*. Should PreVeil (or a PreVeil customer) discover a cyber incident that affects customer information, the PreVeil information assurance compliance program includes the following:

Cyber Incident Reporting: *Coordinate with the customer to conduct a review and report cyber incidents to DoD at https://dibnet.dod.mil, per paragraph (c) requirements including: a review shall include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts in accordance with applicable laws and regulations on the monitoring, access, use, and disclosure of electronic communications and data. PreVeil is an end-to-end encryption system and PreVeil has no access to customer messages and files stored as encrypted blocks on PreVeil servers. However, the customer can decrypt and access their own messages files and logs via PreVeil eDiscovery/data export features if needed for analysis.*

Malicious Software: *If and when malicious software is discovered and isolated as part of incident review, will submit malicious software to DC3 as instructed in paragraph (d).*

Media Preservation and Protection: *Will preserve and protect images of all known affected information systems identified and all relevant monitoring data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest per paragraph (e).*

Access to Additional Information: *Upon request from the DoD, will grant access to additional information or equipment to support a forensic analysis per paragraph (f).*

Cyber Incident Damage Assessment: *If the client or the DoD elects to conduct a damage assessment, will provide all the information collected in the incident review and media preservation activities conducted under paragraphs (c) and (e), to assist in the damage assessment activities upon request under paragraph (g).*

PreVeil maintains a Governance Risk and Compliance (GRC) program that complies with FedRAMP Moderate baseline equivalent under NIST 800-53 and SOC-2, Type 2 certification for all production operations. PreVeil cryptographic module is validated by NIST CSRC under FIPS 140-2.

Randall Battat
CEO, PreVeil, Inc.