CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC0076

SECTION 1 – APPLICANT INFORMATION

Company Name: Stellar Data Recovery Inc.

Address: 48 Bridge Street, Metuchen, New Jersey, 08840, US

General Contact

Name: Abhishek Jain

Phone: 001 844 775 0101

Mobile:

E-Mail: abhishek@stellarinfo.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: Stellar Data Recovery

Version of software: BitRaser Drive Eraser 3.0 & BitRaser Mobile Eraser and Diagnostics 3.0

Version of user manual: 3.0

Algorithm to be used: NIST 800-88 Clear

Please describe the means of deployment for your software/hardware product:

BitRaser Drive Eraser 3.0 software will be delivered in ISO file for erasing drives.
This product doesn't need installation, The ISO file is flashed into the USB to be able to boot a machine to perform drive eraser of connected drive.

BitRaser Mobile Eraser & Diagnostics 3.0 software will be delivered in ISO file for erasing iPhone device.

Stellar will send via email a link to download the ISO file

Please list the equipment you are intending to ship to execute the test, or the means to access/download your software tool:

USB to boot the machine needs to be arranged by ADISA

CLAIMS TESTING APPLICATION FORM

SECTION 3 – MEDIA WHICH YOUR PRODUCT IS TO BE TESTED ON

1 x 256Gb SSD
1 x IPhone 8

ADISA Threat Matrix

RISK LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TEST LEVEL
1 (Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products. Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	**1**
2 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products. Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	**2**
3 (High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	**3**

CLAIMS TESTING APPLICATION FORM

SECTION 4 – THE CLAIM

Stellar software called “BitRaser Drive Eraser v3.0” & “BitRaser Mobile Eraser & Diagnostics v3.0” when used in accordance with user manual 3.0 using NIST 800-88 Purge algorithm will overwrite all user data on the hardware sample within this test to protect to a forensic attack equivalent to test level 1 of the ADISA threat matrix..

I, Abhishek Jain of Stellar confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of Abhishek Jain

SIGNED: **Abhishek Jain**

NAME: Abhishek Jain

TITLE: Sr.Manager - Partner Business

DATE: 26th November 2019

ACCEPTANCE

Claim Accepted by:

Dr Andrew Blyth - ADISA Research Centre

SIGNED:

NAME: Andrew Blyth

TITLE: Director of Research and Technology

DATE: 26.11.2019