CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC0119

SECTION 1 – APPLICANT INFORMATION

Company Name: U-Reach Data Solutions, Inc

Address: 3340 Riverside Dr Ste C Chino, CA 91710 United States

General Contact

Name: Justin Dobrusky

Phone: 9096287030

Mobile:

E-Mail: justin@ureach-usa.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: U-Reach Data Solutions, Inc

Version of software: NV-BM600 Controller PE5232 firmware version 2.5X.XX

Version of user manual: UM-UR-EN-PEV3 V A.04.4

Algorithm to be used: Secure Erase

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

The NV-BM600 duplicator supports 110V/60Hz or 230V/50Hz power sources. Connect the power cord to the duplicator and connect the other end to a proper power source. Flip the switch to start the machine. Once booted, the machine will display the first available function. Plug the desired NVMe SSD drives into any slots 2-6. Using the arrow keys, scroll down to function 4 (Erase) and press OK. Within the submenu, scroll down to function 5 (Secure Erase) and press OK. The operation will begin. The machine will display a green light upon success and indicate success on the LCD screen after the operation is complete. Press the X button to return to the previous menu. The Secure Erase process will take less than 30 seconds. For

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

1x NV-BM600
1 x MTS400-SAS (See ADPC118 for deployment method)

CLAIMS TESTING APPLICATION FORM

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

Digifast ACE M.2 NvME SSD
Kingston A400 SSD

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

NV-BM600 (M.2 and SATA duplicator and sanitizer running firmware Controller PE5232 firmware version 2.5X.XX and when used in accordance with User Manual_UM-UR-EN-PEV3 V A.04.4 and using algorithm Secure Erase, will sanitise all user data on media listed in Section 3, such that forensic techniques aligned to Test Level 2 cannot recover user data.

MTS400-SAS (SAS and SATA duplicator and sanitizer) running firmware Controller HD3970SAS firmware version 2.5X.XX and when used in accordance with User Manual UM-UR&USA-EN-MTS-SAS-20200902 VA.01.4 and using algorithm Full Erase, will sanitise all user data on media listed in Section 3, such that forensic techniques aligned to Test Level 2 cannot recover user data."

I, Justin Dobrusky of UReach Data Solutions, Inc 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 UReach Data Solutions, Inc

SIGNED: 

NAME: Justin Dobrusky

TITLE: Sales and Marketing Manager

DATE: 2021/9/9

ACCEPTANCE

Claim Accepted by:

ADISA Research Centre

SIGNED: 

NAME: Godfred Badu

TITLE: Forensic Analyst

DATE: 10.09.2021