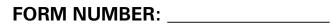
CLAIMS TESTING APPLICATION FORM





SECTION 1 — APPLICANT INFORMATION
Company Name:
Address:
General Contact
Name:
Phone:
Mobile:
E-Mail:
CECTION O APPLICANT COSTWARE INFORMATION
SECTION 2 — APPLICANT SOFTWARE INFORMATION
Manufacturer:
Version of software:
Version of user manual:
Algorithm to be used:
Please describe the means of deployment for your software/hardware product:
Please list the equipment you are intending to ship to execute the test, or the means to access/download your software tool:

CLAIMS TESTING APPLICATION FORM



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

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	
	of confirm	
	ation outlined in this document is an accurate and true reflection of the claims made by our produndergo the ADISA testing method.	duct
Signed on I	behalf of	
SIGNED:	Matt Mickelson	
NAME:		
TITLE:		
DATE:		
ACCEPTAN	ICE	
Claim Acce	epted by:	
SIGNED:	A. H.	
NAME:		
TITLE:		
DATE:	24.02.2021	