EXHIBIT 4

FILED
4 NOV 2013
SUPREME COURT OF NEW SOUTH WALES

Form 40 (version 2)
UCPR 35.1

AFFIDAVIT OF Craig S Wright – 31st Oct 2013

NA

COURT DETAILS

Court	NSW Supreme Court
Division	General Division Common Law
List	General
Registry	Sydney
Case number	2013 / 225983 & 2013 / 245661

TITLE OF PROCEEDINGS

Plaintiff	**Craig Steven Wright (ABN 97 481 146 384)**
Defendant	**W&K INFO DEFENSE RESEARCH LLC**

FILING DETAILS

Filed for	**Craig S Wright** Plaintiff
Contact name and telephone	Craig S Wright 0417 683 914
Contact email	Craig S Wright (craigswright@acm.org)

AFFIDAVIT DETAILS

Name	Craig S Wright
Address	43 St Johns Ave Gordon
Occupation	Director / Lecturer
Date	~~31 Oct 20~~13 4th Novembr 2013

I affirm:

1. I am the plaintiff.

2. I believe that the information contained in this affidavit is true.

3. The defendant is indebted to the plaintiff in respect of the balance of the cause of action 2013 / 225983 for which this action was commenced in the amount of $28,254,666.00 together with interest on the principal sum from the date of the cause of action to today's date of **$156,755.34** calculated as follows:

Period	Days & Rate p.a.	Debt Amount	Interest
25 Jul 2013 – 23 Aug 2013	93 days @ 6.750%	$28,254,666.00	$488,637.81
$5,254.17 per day until entry of judgment			
		Total:	$28,743,303.81

4. The defendant is indebted to the plaintiff in respect of the balance of the cause of action 2013 / 245661 for which this action was commenced in the amount of $28,254,666.00 together with interest on the principal sum from the date of the cause of action to today's date of **$156,755.34** calculated as follows:

Period	Days & Rate p.a.	Debt Amount	Interest
25 Jul 2013 – 23 Aug 2013	93 days @ 6.750%	$28,534,049.79	$490,746.57
$5,254.17 per day until entry of judgment			
		Total:	$29,024,796.36

5. Since the commencement of this action no payments have been made or credits accrued.

6. The amount for filing, issuing and serving of the statement of claim herein, which has not been paid is **$0**.

7. The amount of solicitor's costs calculated in accordance with the Local Courts (Civil Claims) Rules, which has not been paid is $0.

8. The Statement of Claim was served on the defendant on 26 Jul 2013 by leaving it with the Defendant at the registered address for service of:

David A Kleiman
3119 Contego Lane
Palm Beach Gardens
Fl 33410 USA

9. The Statement of Claim was served on the defendant on 26 Jul 2013 by mailing it with the Defendant at the registered mailing address for service of:

David A Kleiman
4371 Northlake Blvd #314
Palm Beach Gardens
Fl 33410 USA

10. The defendant is a US LLC based in Florida USA. The US resident director was David A Kleiman. (Appendix A).

11. The market rate (at this date) for the contract quantity of Bitcoin (Currency Code XBT) on Xe.com is $AUD 67,863,954.23 at a market rate of 1 XBT = 226.213 AUD 1 AUD = 0.00442061 XBT.

12. A contract was formed in April 2011 (Appendix B).

13. 300,000 Bitcoin and a series of software projects was to be paid in 2013 as consideration for this agreement.

14. On 02 Feb 2013 the agreement to pay the 300,000 Bitcoin was noted in an email of Dave Kleiman to Craig Wright noting the verbal agreement to start a Bitcoin exchange based on the mined Bitcoin of Mr Kleiman and the returned amounts paid as consideration.

15. The company, COIN-EXCH PTY. LTD. ACN 163 338 467 was started on 17th Apr 2013 with an agreement for Mr Kleiman to transfer the remaining capital from the contract (B) in repayment as well as to inject a further amount of capital into the company on or before 30th April 2013 Appendix D).

16. The contract was associated with an invoice to be paid for $34,862,323.00 USD from 22Apr 2011. This was paid in full.

17. Mr David A Kleiman died on 26th April 2013 (US time) (Appendix F).

18. The transfers made into “W&K Info Defence LLC” (Appendix G) were completed in April 2013. These are pseudo anonymous but public. The details have been supplied in Appendix G. Details of these transactions have been given to the Australian Tax Office for tax purposes.

19. The Bitcoin addresses used have been independently validated by NSW Solicitors under oath (Appendix H).

20. Work and research was conducted under the US Dept. of Homeland Security DHS BAA

    (a) Appendix I

    (b) Appendix J

    (c) Appendix K

21. Mr Kleiman noted that screening software was developing in unwarranted manners and I noted that our software was looking at being better in an email (Appendix L).

22. The coversheets for the S&T Directorate projects are included in Appendix M

23. On 01st August 2013 a shareholders meeting was called for “W&K Info Defense LLC” to be held on the 16th August 2013. The meeting was emailed to the company address as well as send to the address of the shareholders and company. The shareholding of “W&K Info Defense LLC” was:

1.	Craig S Wright	50.0 %
2.	David A Kleiman	50.0 %

24. The meeting from point 23 meeting was held on the 16th of August 2013. The following people were present:

    1. Jamie Wilson
    2. Craig S Wright

25. “W&K Info Defense LLC” was an incorporated partnership. All shares are held jointly. The constitution states there is to be a resident US director. Shares were held jointly as per the US Companies Act, 1956.

26. The following points were moved at the meeting:

1. Jamie Wilson will act as director for the purposes of consenting to orders and the company to be wound down.

2. The vote was Craig Wright – "Yes". No other parties.

3. It was agreed that following the motion to accept the debt owed by the company (W&K Info Defense LLC), it would be closed.

27. Projects for the development of software started in 2009 under a company named "Integyrs Pty Ltd" (Appendix N).

28. The development of the software was extended considerably in the period between 2011 – 2013.

29. I discovered that Mr Kleiman died before transferring the required funds on the 29th April 2013. The payment was planned for 30th April 2013.

30. Mr Kleiman was not added as a shareholder and director of Coin-Exch Pty Ltd as was planned to occur on the 30th Apr 2013 as a consequence.

AFFIRMED at Sydney ~~Gordon,~~ NSW

Signature of deponent ______________________

Name of witness NICHOLAS CHARLES MCDONALD

Address of witness 21/103 MAJORS BAY ROAD CONCORD NSW 2137

Capacity of witness JUSTICE OF THE PEACE

And as a witness, I certify the following matters concerning the person who made this affidavit (the **deponent**):

I saw the face of the deponent

~~1 I saw the face of the deponent.~~ ~~*[OR, delete whichever option is inapplicable]*~~

2 I have confirmed the deponent's identity using the following identification document:

NSW DRIVERS LICENCE

Identification document relied on (may be original or certified copy)[1]

Signature of witness ______________________

Note: The deponent and witness must sign each page of the affidavit. See UCPR 35.7B.

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174
in and for the State of New South Wales, Australia
21/103 Majors Bay Rd
Concord NSW 2137
Telephone 02 96034779 / 0412 473 696

[[1] "Identification documents" include current driver licence, proof of age card, Medicare card, credit card, Centrelink pension card, Veterans Affairs entitlement card, student identity card, citizenship certificate, birth certificate, passport or see Oaths Regulation 2011 or JP Ruling 003 - Confirming identity for NSW statutory declarations and affidavits, footnote 3.]

A.

Electronic Articles of Organization For Florida Limited Liability Company

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

Article I

The name of the Limited Liability Company is:

W&K INFO DEFENSE RESEARCH LLC

Article II

The street address of the principal office of the Limited Liability Company is:

3119 CONTEGO LANE
PALM BEACH GARDENS, FL. US 33418

The mailing address of the Limited Liability Company is:

4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. US 33410

Article III

The purpose for which this Limited Liability Company is organized is:

ANY AND ALL LAWFUL BUSINESS.

Article IV

The name and Florida street address of the registered agent is:

DAVID A KLEIMAN
3119 CONTEGO LANE
PALM BEACH GARDENS, FL. 33410

Having been named as registered agent and to accept service of process for the above stated limited liability company at the place designated in this certificate, I hereby accept the appointment as registered agent and agree to act in this capacity. I further agree to comply with the provisions of all statutes relating to the proper and complete performance of my duties, and I am familiar with and accept the obligations of my position as registered agent.

Registered Agent Signature: DAVE KLEIMAN

This is the annexure marked with the letter 'A' referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S Wright
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 2 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

Article V

The name and address of managing members/managers are:

Title: MGRM
DAVID A KLEIMAN
4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. 33410 US

Article VI

The effective date for this Limited Liability Company shall be:

02/14/2011

Signature of member or an authorized representative of a member

Electronic Signature: DAVE KLEIMAN

I am the member or authorized representative submitting these Articles of Organization and affirm that the facts stated herein are true. I am aware that false information submitted in a document to the Department of State constitutes a third degree felony as provided for in s.817.155, F.S. I understand the requirement to file an annual report between January 1st and May 1st in the calendar year following formation of the LLC and every year thereafter to maintain "active" status.

B

INTELLECTUAL PROPERTY LICENCE FUNDING AGREEMENT

PARTIES

Craig Wright R&D
ABN 97 481 146 384
(Financer)

AND

W&K Info Defense LLC
(Provider)

This is the annexure marked with the letter 'B' referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig SWRIGHT
~~sworn/~~affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 14 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Ref: CEWK01

K C

THIS DEED dated 22nd day of April 2011

BETWEEN

Craig Wright of Craig Wright R&D

(Financer)

And

Dave Kleiman for W & K Info Defense LLC

(Provider)

RECITALS

A. The Financer controls the following Bitcoin (BTC) addresses:

(a) 12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm.

(b) 12C9c9VQLMrLi4Ffzq2wDvwrKnUPaAaNFp.

B. The Provider desires the intellectual property for the permitted use and to extend this for other purposes desirable to both parties.

C. The Provider will use the funding for the development of several software products.

D. The provider will return the loaned finances (in Bitcoin) on or before 01 July 2013 and 30 Dec 2013.

E. The Provider will remain completely confidential on all matters in this deed (including even that family members do not have knowledge of the transaction).

F. The financer will send the following amounts (in Bitcoin) to to following address by 30 April 2011:

(a) 165,140 BTC

(b) 1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

G. The financer will send the following amounts (in Bitcoin) to toe following address by 30 August 2011:

(a) 50,000 BTC

K

(b) 1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

H. The Financer and the Provider wish to record the licence, which has been granted to the Provider to use the intellectual property in accordance with this deed.

I. The Financer is the absolute owner of the entire unencumbered copyright in the works described in the schedule when complete.

J. The Financer has agreed to license the works to the Provider and the Provider has agreed to accept such licence on the following terms and conditions.

K. The provider will fund the software development using Bitcoin.

L. The Financer will provide 1,024 core Xeon and GPU based hardware solution.

(a) It is acknowledged that two SGI ICE XE310 – 512 core hosts have been provided and are in a data centre specified by the provider

(b) The provider will use these systems to mine Bitcoin

(c) The provider expects to earn 12,000 BTC per month using these systems for the period to 30 June 2013

(d) The systems will be hosted in the US at a facility managed by the provider.

M. The provider will pay for the use of the systems and the loan as follows:

(a) 250,000 BTC to be repaid on 30 June 2013

(b) 50,000 BTC to be repaid on 30 Dec 2013

(c) The developed software will be exclusively licensed perpetually to the financer (as of 30 June 2013).

(d) The software may be used but not distributed by the provider.

N. The contract is complete when 300,000 BTC have been repaid.

O. It is agreed that the value of the loan to be repaid is $ AUD 20,000,000 in two parts (for a total of $40,000,000).

P. The server systems will return to the Financer at the completion of the contract.

Q. On default, the contract is to be repaid in full to the financer.

K

OPERATIVE PART

1. Definitions

In this deed:

(a) Business means the business operated by the Provider described as such in the schedule;

(b) Business day means a day, not being a Saturday, Sunday or gazetted public holiday, on which banks are open for commercial business where performance of an obligation under this deed is to take place;

(c) Claim means, in relation to a person, a claim, demand, remedy, suit, injury, damage, loss, cost liability, action, proceeding, right of action, chose in action, claim for compensation or reimbursement or liability incurred by or to be made or recovered by or against the person, however arising and whether ascertained or unascertained, or immediate, future or contingent;

(d) Commencement date means the date so specified in the schedule;

(e) Confidential information means all technical and other information and know how, including all information and know how in any eye or machine readable form or other format, disclosed or given to the Provider from any source in respect of or incidental to:

(i) The product;

(ii) The technology;

K

(iii) The Financer; and

(iv) Any other information disclosed or given to the Provider by the Financer which is declared by the Financer to be confidential information;

(f) Improvements means any improvement, modification, enhancement or derivative of the intellectual property arising during the term;

(g) Intellectual property means:

(i) The confidential information;

(ii) The improvements;

(iii) The patent; and

(iv) The trade mark;

(h) Licence fee means the amount calculated and paid by the Provider to the Financer specified in the schedule;

(i) Notice means a written notice, consent approval, direction, order or other communication;

(j) Obligation means any legal, equitable, contractual, statutory or other obligation, deed, covenant, commitment, duty, undertaking or liability;

(k) Patent means the registered patent or patent application including the provisional and complete specifications described in the schedule;

(l) Permitted use means to conduct the business to exploit market, promote, develop, integrate, research, sell and conduct and any other activity undertaken with respect to the product for profit or reward;

(m) Product means the product described as such in the schedule;

(n) Right includes a legal, equitable, contractual, statutory or other right, power, authority, benefit, privilege, remedy, discretion or cause of action;

(o) Technology means all that technical information which relates to or forms part of the product, including, without limitation, methodology, techniques, drawings, outlines, notes, algorithms, detailed designs, flow charts, results, software: partial or intermediate versions and prototypes, data, formulae and other proprietary information and know how in the Provider's possession or control or which is revealed to the Provider which relates to the product;

(p) Term means the term set out in the schedule; and

(q) Trade mark means the registered trade mark, trade mark registration application and common law trademarks described in the schedule.

2. Interpretation

This deed is governed by the law of NSW and the parties submit to the non-exclusive jurisdiction of the courts of that state.

In the interpretation of this deed:

(a) References to legislation or provisions of legislation include changes or re-enactments of the legislation and statutory instruments and regulations issued under the legislation;

(b) Words denoting the singular include the plural and vice versa; words denoting individuals or persons include bodies corporate and vice versa; references to documents or deeds also mean those documents or deeds as changed, novated or replaced, and words denoting one gender include all genders;

(c) Grammatical forms of defined words or phrases have corresponding meanings;

(d) Parties must perform their obligations on the dates and times fixed by reference to the schedule;

(e) Reference to an amount of money is a reference to the amount in the lawful currency of the Commonwealth of Australia;

(f) If the day on or by which anything is to be done is a Saturday, a Sunday or a public holiday in the place in which it is to be done, then it must be done on the next business day;

(g) References to a party are intended to bind their executors, administrators and permitted transferees; and

(h) Obligations under this deed affecting more than one party bind them jointly and each of them severally.

3. Licence

The Financer hereby grants to the Provider an exclusive licence to use the intellectual property for the permitted use on the terms of this deed.

In consideration of the licence fee payable hereunder the Financer grants to the Provider an exclusive transferrable licence to copy publish sell or otherwise use the works in the course of its business in Australia and/or Overseas in respect of the whole or any part of the works commencing on 01st July 2013.

In consideration of the licence hereby granted to the Provider the Provider must pay a one off licence fee of $20,000,000 (GST exclusive) to the Financer on or before the 30th June 2013. The provider will also transfer the designated account of the provider:

(a) 250,000 BTC to be repaid on 30 June 2013

(b) 50,000 BTC to be repaid on 30 Dec 2013

The payment is to be issued in Bitcoin as per the schedule.

4. **Provider's promises**

(a) **Undertakings**

The Provider undertakes to:

(i) Use its reasonable commercial endeavours to:

(1) Preserve the value and validity of the intellectual property; and

(2) Create, promote, retain, and enhance the goodwill in the intellectual property;

(ii) During the term and thereafter the termination of this deed not to allow or facilitate the use, nor exploit the intellectual property in a manner in any way detrimental to the Financer and not contravene, deny or contest the rights subsisting in the intellectual property, and take such steps as may be appropriate and available to the Provider to prevent the infringement of any and all the rights subsisting in the intellectual property;

(iii) In connection with the permitted use not give any warranty:

(1) Beyond that which the Provider is obliged in law to give; or

(2) Which has not been approved in writing by the Financer;

(iv) To use the intellectual property only for the permitted use and not for any other use;

(v) Treat as confidential the confidential information except that which at the time of its disclosure to the Provider was generally available, or subsequently became known to the public provided always that this covenant shall continue in full force and effect notwithstanding that this deed has terminated; and

(vi) Devote all reasonable commercial endeavours in the conduct and operation of the business.

(b) **Indemnity**

(i) The Provider hereby agrees to fully, effectually, and promptly indemnify the Financer against any loss, either direct or indirect, damage or expense whatsoever which the Financer may suffer or incur in respect of:

(1) Any breach by the Provider of the provisions of this deed; or

(2) Any claim by any person against the Financer arising out of or in respect of the exploitation of the intellectual property by the Provider; and

(ii) The Provider hereby irrevocably releases the Financer and waives all claims which the Provider may have in the future against the Financer, in respect of any action claim or remedy whatsoever in any way attributable to the exploitation of the intellectual property by the Provider.

5. Improvements

If the Provider develops any improvements, the Financer hereby irrevocably:

(a) Grants to the Provider the right to apply for any incidental intellectual property rights available in respect of that improvement and in connection with such application, the Financer shall:

(i) Make, supply and assist in the preparation of all models, plans, drawings or specifications necessary or convenient for the proper understanding or development of the improvements; and

(ii) Grant and do all things necessary to give effect to an assignment of the intellectual property rights in respect of the improvements to the Provider;

(b) Assigns, transfers and sets over absolutely to the Provider all right title and interest to the improvements including all claims as they relate to the improvements.

6. GST

(a) GST means a goods and services tax as defined in A New Tax System (Goods and Services Tax) Act 1999.

(b) In respect of any taxable supply, the Provider must pay to the Financer an additional amount equal to the prevailing GST rate on the supply. The additional amount referred to in this clause is payable at the same time and in the same manner as the licence fee subject to the receipt by the Provider of a valid tax invoice, as defined in A New Tax System (Goods and Services Tax) Act 1999.

7. Term and termination

(a) Term

This deed begins on 01st July 2013 the commencement date and will continue for the term unless it is earlier terminated.

(b) Termination on notice

Either party may terminate this deed by notice in writing to the other if the other party commits any breach of any provision of this deed, and has failed to remedy such breach within fourteen days of receipt of notice specifying:

(i) The exact nature of the breach committed by the defaulting party; and

(ii) What is required by the defaulting party to remedy the breach;

8. Licence fee

(a) Payment of licence fee

The Provider must pay the licence fee specified in the schedule to the Financer during the term.

(b) Late payment

If the licence fee or any other monies payable by the Provider to the Financer remain unpaid for seven days after the due date for payment, whether or not formal demand has been made, then the Provider shall pay, in addition to any monies actually owing to the Financer, interest at the rate of 2% over the bank indicator lending rate nominated by the Financer on such monies from the date the payment actually fell due until such monies are recovered and paid to the Financer.

9. Warranties by Financer

The Financer warrants to the Provider that:

(a) The Financer has the power and authority to enter into this deed; and

(b) The intellectual property rights granted under this deed will not when used in accordance with this deed infringe the intellectual property rights of any person.

10. Third party claim

(a) Provided that the Provider is not in breach of its obligations under this deed, if a third party makes a claim against the Provider alleging that use of the intellectual property infringes its intellectual property rights, the Financer will defend, indemnify and hold harmless the Provider from such a claim provided that the:

(i) The Provider notifies the Financer in writing promptly of the claim;

(ii) The Provider provides such information, assistance and co-operation as the Financer may reasonably request and at its expense, from time to time; and

(iii) The Financer has full discretion to defend, compromise or settle any such claim on such terms as the Financer deems fit.

(b) If the Financer cannot satisfactorily settle the claim so as to retain ownership of the intellectual property, its liability will be limited to terminating this deed, and refunding the Provider an amount equal to the portion of any licence fee paid for the period following termination.

(c) Nothing in this clause authorises the Provider to defend, compromise or settle any claim on the Financer's behalf.

11. Limitation of liability

(a) Other than in respect of a party's:

(i) Breach of the confidentiality provisions of this deed; or

(ii) Infringement of another party's intellectual property rights; or

(iii) Indemnification obligations under this deed; or

(iv) Wilful misconduct.

(b) Neither party will be liable to the other for any consequential, special or punitive damages arising out of this deed. Each party's cumulative direct damages will be limited to the licence fee payable under this deed in the prior twelve month period. This clause survives the termination or expiration of this deed.

12. Assignment

No party may assign its rights or obligations under this deed without the prior written consent of the other parties, which consent may be given or withheld, or given on conditions, in the absolute discretion of those other parties.

13. Time

The parties hereto agree that time shall in all respects be of the essence in regards this deed.

14. Notices

A communication required by this deed, by a party to another, must be in writing and may be given to them by being:

(a) Delivered personally; or

(b) Posted to their address specified in this deed, or as later notified by them, in which case it will be treated as having been received on the second business day after posting; or

(c) Faxed to the facsimile number of the party with acknowledgment of receipt received electronically by the sender, when it will be treated as received on the day of sending, or

(d) Sent by email to their email address, when it will be treated as received on that day.

15. Waiver or variation

(a) A party's failure or delay to exercise a power or right does not operate as a waiver of that power or right.

(b) The exercise of a power or right does not preclude:

(i) Its future exercise; or

(ii) The exercise of any other power or right; or

(iii) The variation or waiver of a provision of this deed or a party's consent to a departure from a provision by another party will be ineffective unless in writing executed by the parties.

16. Counterpart

This deed may be executed in any number of counterparts each of which will be an original, but counterparts together will constitute one and the same instrument, and the date of the deed will be the date on which it is executed by the last party.

17. Costs

(a) Each party will pay its own costs of and incidental to this deed.

(b) The Provider will bear all duty payable on this deed and keep indemnified the Financer in respect of that liability.

(c) The Provider will bear all GST payable in respect of any supply under this deed upon receipt of tax invoice issued by the Financer.

18. Escrow

(a) The paper Bitcoin Wallet with address 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a will be held by the financer as assurance or the contract and will convert to the ownership of the financer on default of the provider.

(b) All source code and agreements are to be held in a manner that the financer can access on default.

REFERENCE SCHEDULE

Deed date:	01st April 2011
Licence fee:	(a) 250,000 BTC to be repaid on 30 June 2013 (b) 50,000 BTC to be repaid on 30 Dec 2013 (ex GST) for exclusive perpetual assignment
Product:	Bitcoin and Exchange Software in C/C++/C#/R code
Commencement date:	01st July 2011
Term:	Two (2) years
Trademark:	All Marks Associated with C01N and associated marks To be filed K
Patent:	All IP under BAA-001 / 002 / 003 / 004 C

SIGNED AS A DEED

Executed by
W & K Info Defense LLC)
in accordance with s.127)
Corporations Act 2001 (CTH) and its constitution)

Dave Kleiman

Dave Kleiman
DIRECTOR

Executed by
Craig Wright R&D (A.B.N. 97 481 146 384)

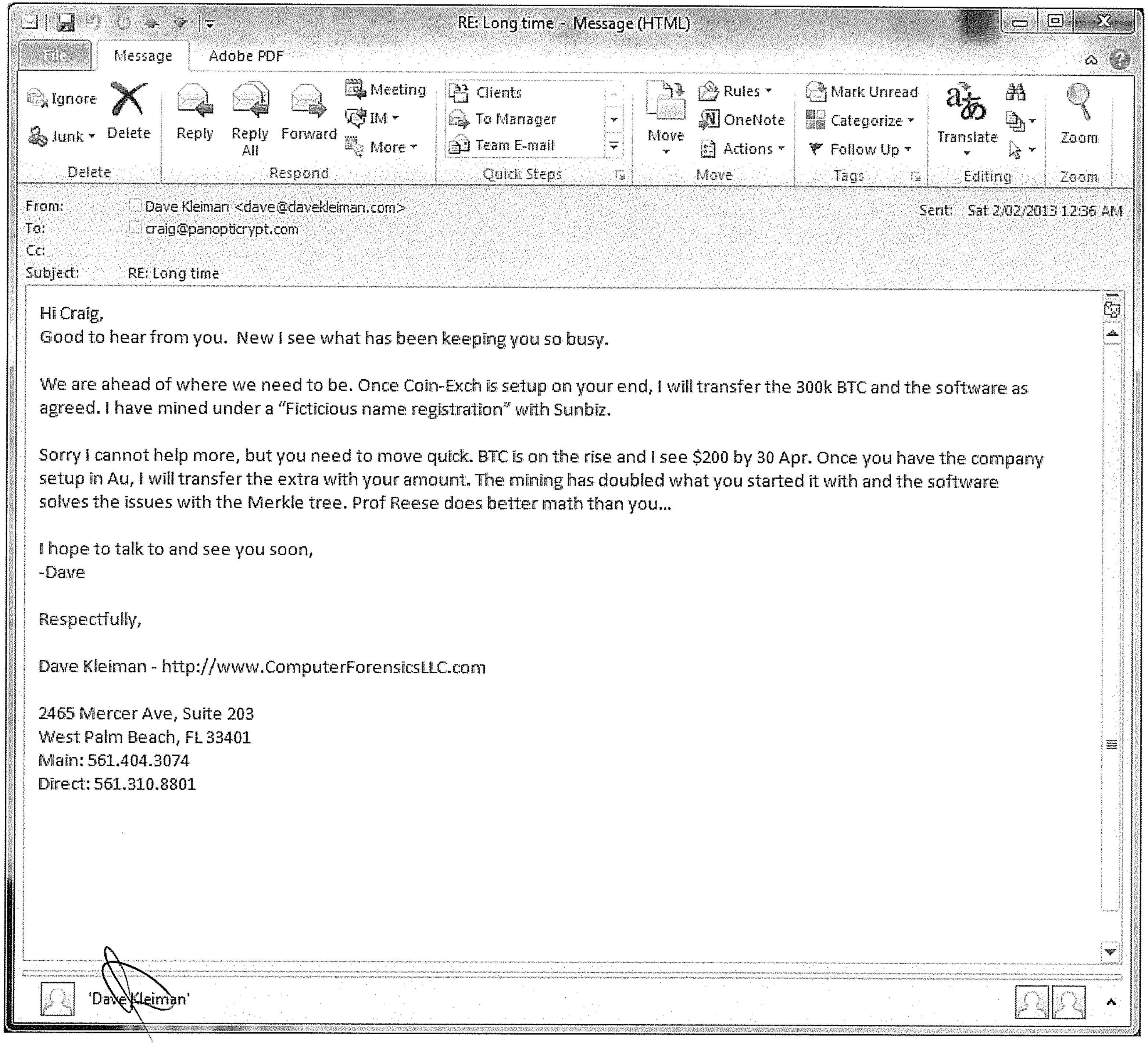
Craig S Wright

C

This is the annexure marked with the letter C referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2013

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174



From: Dave Kleiman <dave@davekleiman.com>
To: craig@panopticrypt.com
Cc:
Subject: RE: Long time
Sent: Sat 2/02/2013 12:36 AM

Hi Craig,
Good to hear from you. New I see what has been keeping you so busy.

We are ahead of where we need to be. Once Coin-Exch is setup on your end, I will transfer the 300k BTC and the software as agreed. I have mined under a "Ficticious name registration" with Sunbiz.

Sorry I cannot help more, but you need to move quick. BTC is on the rise and I see $200 by 30 Apr. Once you have the company setup in Au, I will transfer the extra with your amount. The mining has doubled what you started it with and the software solves the issues with the Merkle tree. Prof Reese does better math than you...

I hope to talk to and see you soon,
-Dave

Respectfully,

Dave Kleiman - http://www.ComputerForensicsLLC.com

2465 Mercer Ave, Suite 203
West Palm Beach, FL 33401
Main: 561.404.3074
Direct: 561.310.8801

'Dave Kleiman'

ASIC
Australian Securities & Investments Commission

Forms Manager
Company Officeholders

Company: COIN-EXCH PTY. LTD. ACN 163 338 467

Company details

Date company registered	17-04-2013
Company next review date	17-04-2014
Company type	Australian Proprietary Company
Company status	Registered
Home unit company	No
Superannuation trustee company	No
Non profit company	No

Registered office

LEVEL 5 , 32-38 DELHI ROAD , MACQUARIE PARK NSW 2113

Principal place of business

LEVEL 5 , 32-38 DELHI ROAD , MACQUARIE PARK NSW 2113

Officeholders

WRIGHT, CRAIG STEVEN
Born 23-10-1970 at BRISBANE QLD
43 ST JOHNS AVENUE , GORDON NSW 2072
Office(s) held: Director, appointed 17-04-2013
Secretary, appointed 17-04-2013

This is the annexure marked with the letter D referred to in the Affidavit / ~~Affirmation/ Statutory Declaration~~ of Craig S WRIGHT
sworn/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2017

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Company share structure

Share class	Share description	Number issued	Total amount paid	Total amount unpaid
FOU	FOUNDERS	21500000	21500000.00	0.00
ORD	ORDINARY	20000000	20000000.00	0.00

Members

PANOPTICRYPT PTY LTD 43 ST JOHNS AVENUE , GORDON NSW 2072

Share class	Total number held	Fully paid	Beneficially held
ORD	17000000	Yes	No

DENARIUZ SG 108 NAMLY AVE , SINGAPORE , SINGAPORE

Share class	Total number held	Fully paid	Beneficially held
ORD	3000000	Yes	Yes

WRIGHT , CRAIG STEVEN 43 ST JOHNS AVENUE , GORDON NSW 2072

Share class	Total number held	Fully paid	Beneficially held
FOU	21500000	Yes	No

INVOICE

E

Date: 4/22/2011
Invoice # 1253

W&K INFO DEFENSE RESEARCH LLC
4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS
FL 33410
561.310.8801
dave@davekleiman.com

Craig Wright R&D
ABN 97 481 146 384
51 Cowangarra Rd
Bagnoo NSW 2446
+61 417 683 914
Customer ID CWR001

Craig Wright R&D
ABN 97 481 146 384
51 Cowangarra Rd
Bagnoo NSW 2446
+61 417 683 914
Customer ID CWRD01

Salesperson	Job	Shipping Method	Shipping Terms	Delivery Date	Payment Terms	Due Date
Dave A Kleiman	BAA 001	Software	NA	By Contract	Due on receipt	30 Apr 2011

Qty	Item #	Description	Unit Price	Discount	Line Total
165,140	Bitcoin	BTC loan @ USD 0.88	0.88		145,323
50,000	Bitcoin	BTC loan @ USD 0.88	0.88		44,000
2	SGI System	SGI ICE XE310 lease	4,411,500		8,823,000
1	Software	Per agreement	20,000,000		20,000,000
	BAA-001	BAA 11-02-TTA 01-0127-WP	650,000		650,000
	BAA-002	BAA 11-02-TTA 09-0049-WP	2,200,000		2,200,000
	BAA-003	BAA 14-02-TTA 01-0025-WP	1,200,000		1,200,000
	BAA-004	BAA 11-02-TTA 01-0127-WP	1,800,000		1,800,000

Total Discount	
Subtotal	34,862,323
Sales Tax	
Total	34,862,323

Terms in CEWK01

Advanced security and research

Thank you for your business!

This is the annexure marked with the letter E referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT ~~sworn/affirmed/declared~~ before me at Sydney on the 4th day of November 2013

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Dave Kleiman

From Wikipedia, the free encyclopedia

Dave Kleiman (1967 - 2013)[1] was a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events.[2][3][4]

Dave Kleiman	
Born	1967 U.S.
Died	April 26, 2013 Palm Beach Gardens, Florida
Occupation	Forensic Computer Investigator
Website	http://www.davekleiman.com/

Contents

This is the annexure marked with the letter F referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig [illegible]
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 20 13

~~One page only~~
Page 1 of 4 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Computer security & forensics

For a number of years in the 1990s, Kleiman was a sworn law enforcement officer for the Palm Beach County Sheriff's Office (PBSO).[3][4] While there, he attained the rank of detective. Also, while at the PBSO, he worked as a System Security Analyst in the Computer Crimes Division and also helped set up the Computer Forensics Lab.[3][4]

Dave Kleiman is a regular contributor to a wide array of online forums and mailing lists where he assists network engineers and other IT professionals of varying levels in solving their issues, regardless of the level of difficulty involved. Kleiman is also well known as an advisor to engineering professionals in numerous industries.[2][3][4]

Dave also regularly volunteers his time and expertise assisting local and federal law enforcement agencies in cases both domestic and international in scope.

He is the creator of the "one-shot server lockdown utility" S-lok for Microsoft Windows servers.[3][4]

On January 1, 2007 he was named Microsoft MVP for Windows - Security

Publications

- Co-author: Microsoft Log Parser Toolkit; Syngress Publishing; ISBN 1-932266-52-6
- Co-author: Security Log Management: Identifying Patterns in the Chaos; Syngress Publishing; ISBN 1-59749-042-3
- Technical editor: Perfect Passwords: Selection, Protection and Authentication; Syngress Publishing; ISBN 1-59749-041-5
- Technical editor: Winternals Defragmentation, Recovery, and Administration Field Guide; Syngress Publishing; ISBN 1-59749-079-2
- CD and DVD Forensics: Technical Editor, ISBN 1-59749-128-4
- How to Cheat at Windows System Administration: Contributing Author, ISBN 1-59749-105-5
- Enemy at the Water Cooler: Real Life Stories of Insider Threats, Technical Reviewer, ISBN 1-59749-129-2
- Rootkits for Dummies: Technical editor, ISBN 978-0-471-91710-6
- Windows Forensic Analysis Including DVD Toolkit: Technical Editor, ISBN 1-59749-156-X
- The Official CHFI Study Guide (Exam 312-49): Co-Author, ISBN 1-59749-197-7

References

1. ^ "Obituary: Former PBSO deputy dies in his home" (http://www.mypalmbeachpost.com/news/news/local/obituary-former-pbso-deputy-dies-in-his-home/nXcqR/). Palm Beach Post. Retrieved May 1, 2013.
2. ^ a b "SANS WhatWorks Summit in Forensics and Incident Response" (http://www.sans.org/forensics09_summit/speakers.php#kleiman). SANS.
3. ^ a b c d e "Dave Kleiman" (http://credencecorp.com/bios/DaveKleiman.html). CredenceCorp.

4. ^ *a b c d e* "Dave Kleiman" (http://www.oreillynet.com/pub/au/2560?x-t=book.view). O'Reilly.

External links

- Dave Kleiman's personal web site (http://www.davekleiman.com)
- Palm Beach County Sheriff's Office (http://www.pbso.org)
- CastleCops (http://www.castlecops.com)
- Microsoft MVP Program (https://mvp.support.microsoft.com/mvpexecsum)
- Microsoft MVP profile (https://mvp.support.microsoft.com/profile=C4ED32CD-9982-45F2-8636-BDE271C0DAC2)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Dave_Kleiman&oldid=553157307"

Categories: 1967 births | 2013 deaths | People associated with computer security

This page was last modified on 2 May 2013 at 06:28.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy.
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

From: Carter Conrad <carter@computerforensicsllc.com>
Sent: Tuesday, 30 April 2013 1:23 AM
To: Patrick Paige
Cc: Bill Long; Greg Kelley; Craig Ball; Matthew Shannon; Jerry Hatchett; Eric Robi; Greg Freemyer; Paul Henry; Craig S. Wright; Scott Moulton'; Wayne Marney; Bob Bell; Bill Dean; Kimon Andreou; Greg Kelley
Subject: Dave Kleiman

As close friends of Dave, Patrick and I wanted to let you know in advance of any general posting that we have lost a dear friend and colleague…
As most of you are aware Dave was battling an infection from 2010, and had never fully recovered in the 2 ½+ years that followed.
Dave died in his home in Palm Beach Gardens of, what is being told to us, natural causes.
At this time no further details are available, although there are plans for a memorial, and these will be pasted on as they become available.

Carter V Conrad, Jr
Computer Forensics, LLC
1880 N. Congress Avenue, Suite 333
Boynton Beach, Florida 33426
Phone: (561) 404-3074
Cell: (561) 502-3935

www.ComputerForensicsLLC.com

The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and/or work product and as such is privileged and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.

Home Charts Stats Wallet

Bitcoin Address

G

Summary

Address	12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm
Short Link	http://blockchain.info/fb/12hrmm
Tools	Taint Analysis - Related Tags - Unspent Outputs

This is the annexure marked with the letter G referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT ~~sworn/affirmed/declared~~ before me at Sydney on the 4th day of November 2013

~~One page only~~
Page 1 of 8 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Transactions

No. Transactions	2
Total Received	$ 74,055,693.41
Final Balance	$ 0.00

Request Payment Donation Button

Transactions

Filter

ddb352955903db83f76edb85f2121c51859b2f41a3... 2011-08-27 02:29:26

1PWr5e1JjL8wy6uzKzb5d3pCxkNLYm5vt1
1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

$ 74,055,693.41

796187f76168cd0ca2fff6c3f967fe28242429cec320e... 2011-08-27 02:29:26

12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm

$ 74,055,693.41

Home Charts Stats Wallet

Bitcoin Address

Summary

Address	1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7
Short Link	http://blockchain.info/fb/1msuv
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions

No. Transactions	2
Total Received	$ 36,551,156.21
Final Balance	$ 0.00

Request Payment | Donation Button

Transactions

Filter

0121f30f11152b3df11904401e13b1b972a5408682... 2011-04-29 03:20:56

1B4JfdD4jGUWBehtGF2Phb4BxeN2ytkTxh
1GEeroqocswEazxzeNAJh3KPPD7C61XY2H

$ 36,551,156.21

62fec42dd4370e0aeae88b3fe2a9970bb56a8d4bf0c... 2011-04-29 03:20:56

1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

$ 36,551,156.21

Home Charts Stats Wallet

Bitcoin Address

Summary

Address	1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7
Short Link	http://blockchain.info/fb/1msuv
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions

No. Transactions	2
Total Received	165,140 BTC
Final Balance	0.00 BTC

Request Payment Donation Button

Transactions

Filter

0121f30f11152b3df11904401e13b1b972a5408682... 2011-04-29 03:20:56

1B4JfdD4jGUWBehtGF2Phb4BxeN2ytkTxh
1GEeroqocswEazxzeNAJh3KPPD7C61XY2H

-165,140 BTC

62fec42dd4370e0aeae88b3fe2a9970bb56a8d4bf0c... 2011-04-29 03:20:56

1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

165.140 BTC

Home Charts Stats Wallet

Bitcoin Address

Summary

Address	12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm
Short Link	http://blockchain.info/fb/12hrmm
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions

No. Transactions	2
Total Received	334,587.42424242 BTC
Final Balance	0.00 BTC

Request Payment Donation Button

Transactions

Filter

ddb352955903db83f76edb85f2121c51859b2f41a3... 2011-08-27 02:29:26

1PWr5e1JjL8wy6uzKzb5d3pCxkNLYm5vt1
1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

-334,587.42424242 BTC

796187f76168cd0ca2fff6c3f967fe28242429cec320e... 2011-08-27 02:29:26

12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm

34 167 42424242 BTC

This is the annexure marked with the letter 'H' referred to in the [illegible] CRAIG S WRIGHT
~~Affidavit / Statutory Declaration~~ Sydney
~~sworn/affirmed/~~declared before me at
on the 4th day of November 2013

~~One page only~~
Page 1 of 2 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

H.

Statutory Declaration

OATHS ACT 1900, NSW, EIGHTH SCHEDULE

I, Stephen D'Emilio, of Level 3, 2 Bligh Street, Sydney, in the State of New South Wales, Solicitor, do solemnly and sincerely declare that:

1. I am the solicitor acting for Mr Craig Wright and Hotwire Pre-emptive Intelligence Pty Ltd.

2. On 11 October 2013, Mr Wright came into my office and showed me his HTC mobile phone (**Wright mobile**).

3. On the screen of the Wright mobile, I viewed and verified the following Bitcoin wallet addresses:

   (i) 1JzzLXxuwn45S9HvBqAhkhWa3GhyG3zm64;

   (ii) 168Rc6wJdL4chWhEUQwyywi4sHub6erf2s;

   (iii) 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF;

   (iv) 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a; and

   (v) 16cou7Ht6WjTzuFyDBnht9hmvXytg6XdVT (**Bitcoin wallet addresses**).

4. I viewed the Bitcoin wallet addresses by scrolling down the screen on the Wright mobile.

5. It appeared to me that if Mr Wright wanted to, he could control all of, and make transactions in, the Bitcoin wallet addresses.

6. I make this solemn declaration conscientiously believing the same to be true and by virtue of the provisions of the *Oaths Act 1900*.

Declared at Sydney on 11 October 2013

....
Stephen D'Emilio

in the presence of an authorised witness, who states:

I, Adrian Fong, a solicitor certify the following matters concerning the making of this statutory declaration by the person who made it:

(i) I saw the face of the person;

(ii) I have known the person for at least 12 months.

Adrian Fong

11 October 2013

Craig S Wright

From: BAA Program Support Office <dhsbaa@reisys.com>
Sent: Wednesday, 2 March 2011 8:56 AM
To: Craig S. Wright; Craig S. Wright; Craig S. Wright
Subject: BAA BAA 11-02-TTA 09-0049-WP Upload Received

Your upload has been received electronically at the DHS BAA Support Office.

IV

BAA 11-02 Proposal #: BAA 11-02-TTA 09-0049-WP
Proposal Title: Risk Quantification
Company Name: W&K INFO DEFENSE RESEARCH LLC

White Paper Uploaded on: 03/01/11 04:55 PM EST
File Name: BAA 11-02-TTA 09-0049-WP Risk Quantification.pdf
File Type: Portable Document Format
File Size: 357845 bytes

Uploaded by: Craig S. Wright

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

This is the annexure marked with the letter 'I' referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT
~~sworn/affirmed~~/~~declared~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 4 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

From: BAA Program Support Office <dhsbaa@reisys.com>
Sent: Wednesday, 2 March 2011 9:00 AM
To: Craig S. Wright; Craig S. Wright; Craig S. Wright
Subject: BAA BAA 11-02-TTA 01-0127-WP Upload Received

Your upload has been received electronically at the DHS BAA Support Office.

BAA 11-02 Proposal #: BAA 11-02-TTA 01-0127-WP
Proposal Title: Software Assurance through Economic Measures
Company Name: W&K INFO DEFENSE RESEARCH LLC

White Paper Uploaded on: 03/01/11 04:59 PM EST
File Name: BAA 11-02-TTA 01-0127-WP Software Assurance through Economic Measures.pdf
File Type: Portable Document Format
File Size: 290708 bytes

Uploaded by: Craig S. Wright

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

Craig S Wright

From: BAA Program Support Office <dhsbaa@reisys.com>
Sent: Wednesday, 2 March 2011 10:46 AM
To: Wright, Craig S. ; Wright, Craig S. ; Wright, Craig S.
Subject: Submission confirmation of your DHS BAA Program Proposal # BAA 11-02-TTA 01-0127-WP

Your proposal has been received electronically at the DHS Program Support Office.

BAA 11-02 White Paper Proposal #: BAA 11-02-TTA 01-0127-WP
Proposal Title: Software Assurance through Economic Measures
Company Name: W&K INFO DEFENSE RESEARCH LLC

Proposal Details:
Cover Sheet A completed on: 02/16/11 02:33 AM EST
Cover Sheet B completed on: 02/16/11 12:50 AM EST
White Paper Upload completed on: 03/01/11 04:59 PM EST
File Name: BAA 11-02-TTA 01-0127-WP Software Assurance through Economic Measures.pdf
File Type: Portable Document Format
File Size: 283 KB bytes

Submitted electronically by: Wright, Craig S.

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

Craig S Wright

From: BAA Program Support Office <dhsbaa@reisys.com>
Sent: Wednesday, 2 March 2011 10:53 AM
To: Wright, Craig S. ; Wright, Craig S. ; Wright, Craig S.
Subject: Submission confirmation of your DHS BAA Program Proposal # BAA 11-02-TTA 09-0049-WP

Your proposal has been received electronically at the DHS Program Support Office.

BAA 11-02 White Paper Proposal #: BAA 11-02-TTA 09-0049-WP
Proposal Title: Risk Quantification
Company Name: W&K INFO DEFENSE RESEARCH LLC

Proposal Details:
Cover Sheet A completed on: 02/16/11 02:30 AM EST
Cover Sheet B completed on: 02/16/11 01:22 AM EST
White Paper Upload completed on: 03/01/11 04:55 PM EST
File Name: BAA 11-02-TTA 09-0049-WP Risk Quantification.pdf
File Type: Portable Document Format
File Size: 349 KB bytes

Submitted electronically by: Wright, Craig S.

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

Skip Navigation
Contact Us

Homeland Security

BAA Program

J.

DHS Broad Agency Announcements (BAA) Program Portal

BAA Home

- Basic Research Focus Areas
- High Priority Technology Areas
- Solicitations
  - Current Solicitations
  - Past Solicitations
  - Solicitation Awards
  - **Proposal Submission**
  - Awardee Portal
  - News And Events
  - S&T Directorate Events
  - ST Directorate SBIR Website
  - Privacy Policy
  - FAQs
  - Program Portal

Registration Form

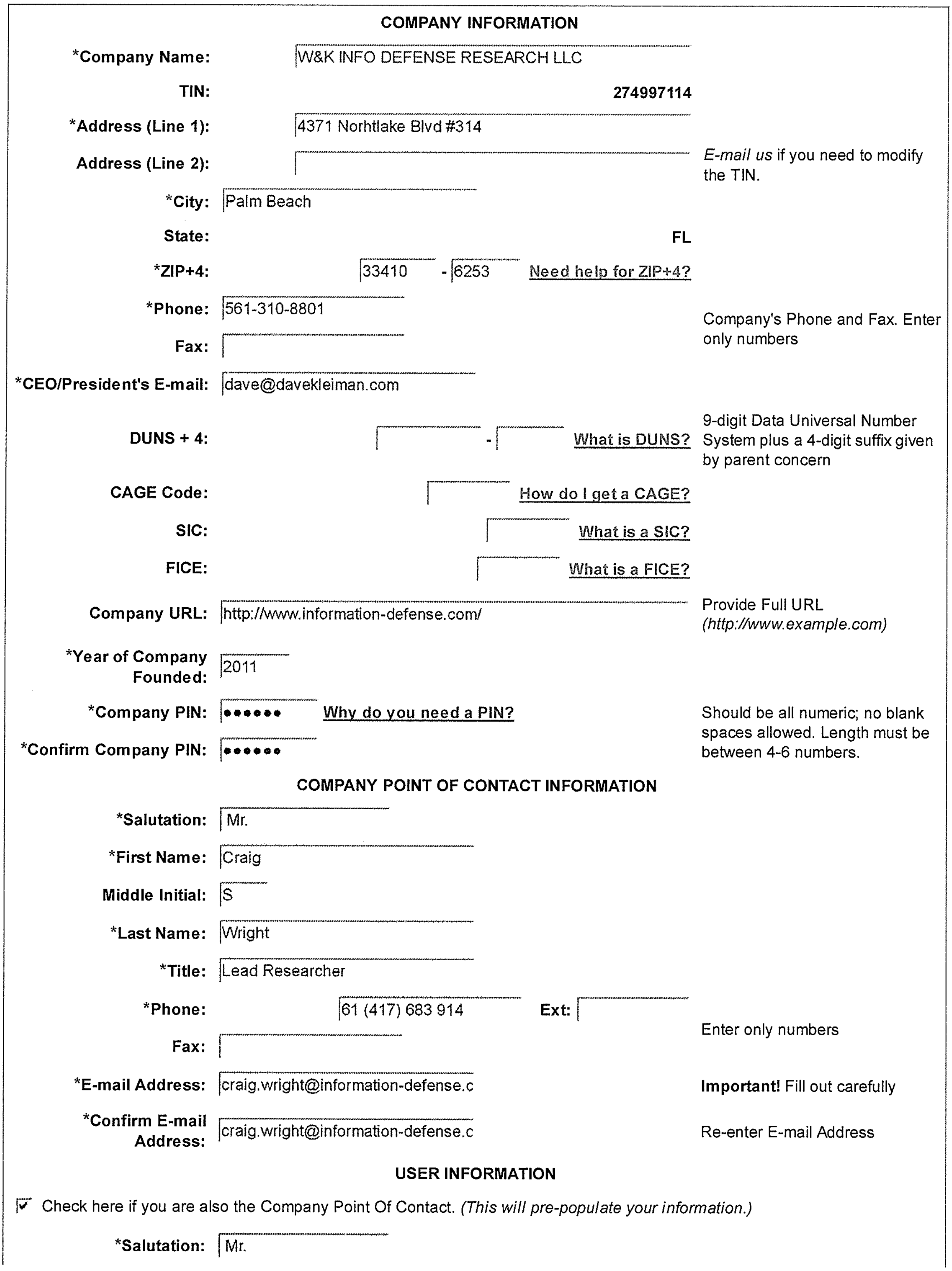
Please do not register yourself MORE THAN ONCE!

Fill in your registration information below. If there are errors on the registration form, you will be asked to re-enter the Company PIN and user password. **(Note: For security reason, this page will expire after 20 minutes of inactivity.)**

Re(g)ister Back

*** Required Information**

This is the annexure marked with the letter J referred to in the Affidavit / ~~Affirmation / Statutory Declaration of~~ Greg S WRIGHT
~~sworn~~/affirmed/~~declared before~~ me at Sydney
on the 4th day of November 2013
~~One page only~~
Page 1 of 6 pages
NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174



COMPANY INFORMATION

*Company Name: W&K INFO DEFENSE RESEARCH LLC

TIN: 274997114

*Address (Line 1): 4371 Norhtlake Blvd #314

Address (Line 2):

E-mail us if you need to modify the TIN.

*City: Palm Beach

State: FL

*ZIP+4: 33410 - 6253 Need help for ZIP+4?

*Phone: 561-310-8801

Fax:

Company's Phone and Fax. Enter only numbers

*CEO/President's E-mail: dave@davekleiman.com

DUNS + 4: - What is DUNS?

9-digit Data Universal Number System plus a 4-digit suffix given by parent concern

CAGE Code: How do I get a CAGE?

SIC: What is a SIC?

FICE: What is a FICE?

Company URL: http://www.information-defense.com/

Provide Full URL *(http://www.example.com)*

*Year of Company Founded: 2011

*Company PIN: •••••• Why do you need a PIN?

*Confirm Company PIN: ••••••

Should be all numeric; no blank spaces allowed. Length must be between 4-6 numbers.

COMPANY POINT OF CONTACT INFORMATION

*Salutation: Mr.

*First Name: Craig

Middle Initial: S

*Last Name: Wright

*Title: Lead Researcher

*Phone: 61 (417) 683 914 Ext:

Fax:

Enter only numbers

*E-mail Address: craig.wright@information-defense.c

Important! Fill out carefully

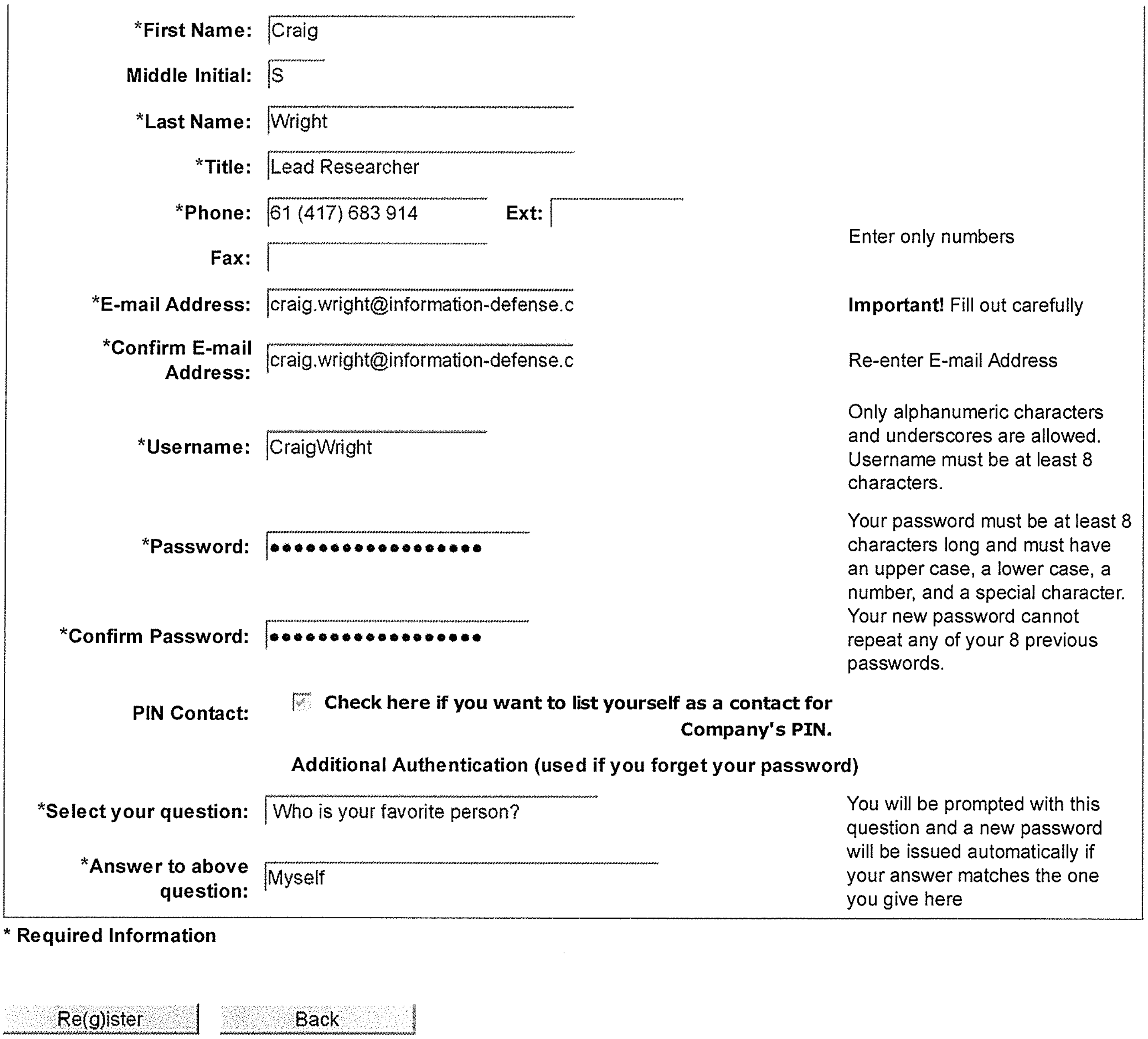
*Confirm E-mail Address: craig.wright@information-defense.c

Re-enter E-mail Address

USER INFORMATION

☑ Check here if you are also the Company Point Of Contact. *(This will pre-populate your information.)*

*Salutation: Mr.



*First Name: Craig

Middle Initial: S

*Last Name: Wright

*Title: Lead Researcher

*Phone: 61 (417) 683 914 Ext:

Fax:

Enter only numbers

*E-mail Address: craig.wright@information-defense.c

Important! Fill out carefully

*Confirm E-mail Address: craig.wright@information-defense.c

Re-enter E-mail Address

*Username: CraigWright

Only alphanumeric characters and underscores are allowed. Username must be at least 8 characters.

*Password: ●●●●●●●●●●●●●●●●●●

*Confirm Password: ●●●●●●●●●●●●●●●●●●

Your password must be at least 8 characters long and must have an upper case, a lower case, a number, and a special character. Your new password cannot repeat any of your 8 previous passwords.

PIN Contact: ☑ **Check here if you want to list yourself as a contact for Company's PIN.**

Additional Authentication (used if you forget your password)

*Select your question: Who is your favorite person?

*Answer to above question: Myself

You will be prompted with this question and a new password will be issued automatically if your answer matches the one you give here

*** Required Information**

DHS Form 10025 (7/07)

- U.S. Department of Homeland Security
- Science & Technology
- S&T Directorate SBIR Website
- OSDBU
- SAFETY Act
- SECURE Program
- Contact Us

Craig S Wright

From:	Dave Kleiman <dave@davekleiman.com>
Sent:	Wednesday, 16 February 2011 2:22 PM
To:	craig.wright@Information-defense.com
Cc:	lynn.wright@information-defense.com
Subject:	RE: Registration - TTA1
Attachments:	W&K Info Defense Research LLC - 08.pdf
Importance:	High

Look over the attached real quickly.

Let me know if it is ok.

Or should the PoC be in the US?? I see a non US vendor on the list.

Pay special attention to "Additional Authentication"

Dave

-----Original Message-----
From: Craig S Wright [mailto:craig.wright@information-defense.com]
Sent: Tuesday, February 15, 2011 22:04
To: Dave Kleiman
Subject: RE: Registration - TTA1

51 Cowangarra Rd
Bagnoo, New South Wales, 2446
AU

The other is not any longer

-----Original Message-----
From: Dave Kleiman [mailto:dave@davekleiman.com]
Sent: Wednesday, 16 February 2011 1:08 PM
To: craig.wright@Information-defense.com; lynn.wright@information-defense.com
Subject: RE: Registration - TTA1

Are either of these your current address?

51 Cowangarra Rd
Bagnoo, New South Wales, 2446
AU

Level 19, 2 Market Street
Sydney, NSW 2000

AU

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 14:13
To: 'craig.wright@Information-defense.com'; 'lynn.wright@information-defense.com'
Subject: RE: Registration - TTA1

It is under vendor registration that it requested DUNS see:
https://www.fbo.gov/?s=main&mode=list&tab=register&subtab=step1

Dave

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 07:29
To: 'craig.wright@Information-defense.com'; 'lynn.wright@information-defense.com'
Subject: RE: Registration - TTA1
Importance: High

Last page of attached. Do you think I can list you as mgr or mgrm with a foreign address, or you think they would kick it back?

Dave

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 06:35
To: 'craig.wright@Information-defense.com'; lynn.wright@information-defense.com
Subject: RE: Registration - TTA1

Did you already create a username and password?

-----Original Message-----
From: Craig S Wright [mailto:craig.wright@information-defense.com]
Sent: Tuesday, February 15, 2011 04:48
To: Dave Kleiman; lynn.wright@information-defense.com
Subject: Registration - TTA1

The first is to do with the attached papers...

TTA 01
<https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#0> - Software Assurance

White paper title Software assurance through economic measures

This also leads to the following one with:

TTA 14 <https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#13> - Software Assurance MarketPlace (SWAMP)

White paper title Software derivative markets

And

Information Security risk markets

Greyfog (last email) should also come under TTA 05 <https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#4> - Secure, Resilient Systems and Networks

...

Dr. Craig S Wright <http://gse-compliance.blogspot.com/> GSE-Malware, GSE-Compliance, LLM, & ...

Information Defense <http://www.information-defense.com/> Pty Ltd

Mobile: 0417 683 914

Description: Logo4

This is the annexure marked with the letter 'K' referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT ~~sworn/affirmed/declared~~ before me at Sydney on the 4th day of November 2013

~~One page only~~
Page 1 of 41 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

K

Proposal White Paper	**(Type I)**
BAA number, •	BAA 11-02-TTA 01-0127-WP
Title of proposal;	Software Assurance through Economic Measures
Name of offeror	W&K INFO DEFENSE RESEARCH LLC
Administrative Contact:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
Technical Contact:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and an Australian Research Company.

Amount Requested (in dollars):	$650000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

1.1 Related Work

Other studies of coding processes and reliability have been conducted over the last few decades. The majority of these have been based either on studies of large systems and mainframe based operations or have analyzed software vendors. In the few cases where coding practices within individual organization have been quantitatively analyzed, the organizations have been nearly always large telecommunications firms or have focused on SCADA and other critical system providers.

Whilst these results are extremely valuable, they fail to reflect the state of affairs within the vast majority of organizations. With far more small to medium businesses coupled with comparatively few large organizations with highly focused and dedicated large scale development teams (as can be found in any software vendor), an analysis of in-house practice is critical to both security and the economics of in-house coding.

As the Internet becomes all persuasive, internal coding functions are only likely to become more prevalent and hence more crucial to the security of the organization.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as exist in short sales of stocks). The first contract would be taken by a user and would pay a fixed amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.

This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.

Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.

This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

Utility to Department of Homeland Security

The game theoretic approach to this can be modeled looking at the incentives of the business and programming functions in the organization. Programmers are optimists. As Brooks noted, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development.

Technical Approach

Just as car dealers buff the exterior and detail the upholstery of a used car, neglecting the work that should be done on the engine, software vendors add features. Most users are unlikely to use even a small fraction of these features, yet they buy the product that offers more features over the more secure product with fewer features. The issue here is that users buy the features over security. This is a less expensive option for the vendor to implement and provide.

The creation of a security and risk derivative should change this. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs. This would most likely lead to product differentiation (as occurred in the past with Windows 95/Windows NT). Those businesses who wish to pay for security could receive it. Those wanting features would get what they asked for.

It is argued that software developers characteristically do not correct all the security vulnerabilities and that known ones remain in the product after release. Whether this is due to a lack of resources or other reasons, this is unlikely to be the norm and would be rectified by the market. The cost of vendors in share price and reputational losses exceed the perceived gains from technical reasons where the fix might break existing applications. The application is already broken in the instance of a security vulnerability.

Users could still run older versions of software and have few, if any, bugs. The issue is that they would also gain no new features. It is clear that users want features. They could also choose to use only secure software, but the costs of doing so far outweigh the benefits and do not provide a guarantee against the security of a system being compromised. As such, the enforced legislation of security standards against software vendors is detrimental. A better approach would be to allow an open market based system where vendors can operate in reputational and derivative markets.

At the end of any analysis, security is a risk function and what is most important is not the creation of perfectly security systems, but the correct allocation of scarce resources. Systems need to be created that allow the end user to determine their own acceptable level of risk based on good information.

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

<u>This work and research follows and continues that published as:</u>

> Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China

Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and Implication", ISBN 1616928050 and 9781616928056, Information Science Publishing, July 2010.

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

"Challenges Faced by the SCADASEC Mailing List", Protecting Canada's Critical Infrastructure 2010 Control Systems Security Workshop, sponsored by Royal Canadian Mounted Police (Ontario Technological Crime), Public Safety Canada and Emergency Management Ontario (Critical Infrastructure Assurance Program), Wednesday April 14, 2010 and Thursday, April 15, 2010.
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
Author of "Critical Infrastructure: Homeland Security and Emergency Preparedness", Second Edition, ISBN 1420095277 and 9781420095272, Taylor & Francis CRC Press, December 2009.
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
Contributor (introduction speaker) of "The Year in Homeland Security", 2008/2009 Edition (Charles Oldham, editor director), Faircount Media Group.
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
Author (co-author) of "Transportation Systems Security", ISBN 1420063782 and 9781420063783, Taylor and Francis CRC Press, May 2008.
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

Costs, Work, and Schedule

Amount Requested (in dollars):	$650,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

• PhD Funding	$240,000
• Supervision	$180,000
• Survey and data Analysis	$230,000

BAA Number: BAA 11-02-TTA 01-0127-WP
Offeror Name: W&K INFO DEFENSE RESEARCH LLC
Title Software Assurance through Economic Measures
Date: 07/04/2010

N/A

Operational Capability:
The project will analyze a sample of at least 1,000 coding projects using existing static analysis tools, manual code review and related techniques. Where these methods are lacking, proposals and methods to integrate existing methods and to fill the gaps left will be created.

Proposed Technical Approach:
This project will address and provide measures and The analysis will measure the following coding errors:

- Format string errors
- Integer Overflows
- Buffer overruns
- SQL Injection
- Cross-Site scripting
- Race Conditions
- Command Injection.

Several published papers have been released (forthcoming include)

> Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

> Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Schedule, Cost, Deliverables, & Contact Info:
Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.

Deliverables:
20-30 published papers
3 PhD Thesis' in the field
A commercial model for software derivatives and insurance markets

A means to measure and predict the following coding errors is being developed

Format string errors
Integer Overflows
Buffer overruns
SQL Injection
Cross-Site scripting
Race Conditions
Command Injection.

Corporate Information:
Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253

Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

Proposal White Paper **(Type I)**

BAA number, •	BAA 11-02-TTA 09-0049-WP
Title of proposal;	Risk Quantification
Name of offeror	W&K INFO DEFENSE RESEARCH LLC
Administrative Contact:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
Technical Contact:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

Amount Requested (in dollars):	$2,200,000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

Using empirical evidence, this research aims to investigate and quantify the root cause of security flaws that act as a source of system compromise. Research into the effects of poor system design, market based risk solutions based on derivative instruments and the impact of common system misconfigurations will be incorporated into multivariate survival models. This research incorporates the economic impact of various decisions as a means of determining the optimal distribution of costs and liability when applied to information security and in particular when assigning costs in computer system security and reliability engineering.

The objective of this research is to produce an innovative modelling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

   a. constant and homogenous failure rates,
   b. binary failure and univariate reliability,
   c. censoring of failure data, and
   d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

To do this, it is necessary to recognise that information security is a risk function (Anderson, Longley & Kwok, 1994). Paying for too much security can be more damaging in economic terms than not buying enough. This leads to decisions about where the optimal expenditure on damage prevention should lie. This research will investigate who should be responsible for the security failures that are affecting the economy and society and how can this be maximized in order to minimize negative externalities (Cohen, 1976). The conclusions will be presented using an empirical study of software hazard rates and audit failures along with the question of how to enforce liability in a global economy.

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

The introduction of Game Theory and Behavioural Economics (Anderson, 2001; Anderson, & Moore, 2006; Varian, 2004) have created a foundation for the rationalisation of information security processes which lead to improved allocation of economic resources. The optimal distribution of economic resources across risk allocations in information system can only lead to a combination of more secure systems for a lower overall cost. This research will incorporate the game theoretic multi-player decision problem. Agents in the model will be deemed to be rational with well-defined preferences, include the ability to reason strategically using their knowledge and belief of other players and to act according to a combination of both economic "*first thought*" and deep strategic thinking (Nissan, et. al., 2007). Solutions to these models will be sought through a combination of the following game devices:

- Equilibrium: evolutive (steady state) games
- Heterogeneous sequential games
- Rationalisability: deductive reasoning

The models will detail the existence of strictly dominating games where these exist in information security practices and propose methods to improve these models. Existing information security practices in existing organisations will be classified into the following game types:

- Non-cooperative vs. cooperative game
- Strategic vs. extensive game
- Perfect vs. imperfect information

Bounded rationality, behavioural game aspects and other feedback effects will be investigated (Nissan, et. al., 2007). Social capital based on fairness and reciprocity will be defined as it applies to the economically efficient application of risk processes associated with Information systems. Contract Theory will be used to explain the creation of agreements and "*contracts*" in the presence of information asymmetry. This is approached through the combination of adverse selection, moral hazards and the "*signalling game*". In this, adverse selection is defined as the "*Principal not having been informed of the other agent's private information ex-ante*" such as in George Akerlof's "*Market for lemons*" (1970). This application of game theory has been asserted to explain many aspects of the software industries predisposition to create insecure software (Anderson, 2001). Arora, Telang and Xu (2004) asserted that a market-based mechanism for software vulnerabilities would necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic *pricing game*. In the model reported, the players in the market do not report their prices[1]. These players use a model where information is distributed simultaneously to the client of the player and the vendor. The CERT model was touted as being the most favourable solution. The research will demonstrate that the examined "*market*" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets that rely on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls. It is to be demonstrated that there are flaws with this approach that can be solved through the creation of a security and risk derivative market for software. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs (Bacon et. al. 2009).

1.2 Our contribution and Technical Approach

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing security vulnerabilities. The goal of this research project is to create a series of quantitative models for information security. Mathematical modelling techniques that

[1] E.g., iDefense Ltd. and other similar providers have a semi-closed market with limited information exchange.

can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modelling,
- Behavioural Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modelling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

This data will be coupled with hazard models created and validated using Honeynets (e.g. Project Honeynet), reporting sites such as the Internet Storm Centre and iDefence. The combination of this information will provide the framework for a truly quantitative security risk framework[2]. At present, the DShield storm centre receives logging from over 600,000 organisations. This represents a larger quantity of data than is used for actuarial data in the home insurance industry. The problem being that this information is not collated or analysed in any quantitatively sound manner. This research will model survival times for types of applications using the body of research into quantitative code analysis for risk. The research will create a series of models (such as those used within mechanical engineering, material science etc) for Information Risk.

Some of the methods that are planned testing in the creation of the risk framework will include:

- Random forest clustering,
- K-means analysis,
- Other classification algorithms, and
- Network associative maps in text analysis forensic work.

The correlation of reference data (such as IP and functional analysis data) between C&C (Command and Control) systems used in "*botnets*" is one aspect of this research. Starting from the outside (the cloud and perimeter) and working inwards to the network, the risk model would start by assessing external threats and move into internal threat sources, becoming gradually become more and more granular as one moves from network to individual hosts and finally to people (user behaviour (Varian, 2004)) and application modelling (Guo, Jarrow, & Zeng, 2005). The eventual result will be the creation of a model that can incorporate the type of organisation, size, location, application, systems used, and the user awareness levels to create a truly quantitative risk model. This would be reported with SE (standard error) and confidence level rather than a point estimate. Code to import data from hosts and networks, using raw "*pcap traces*"[3] will be developed such that system statistics and other data can be collated into a standardised format. This code will be developed in "R" and "C++". This will enable the

[2] Support has been sought and received from SANS (including DShield), CIS (Centre for Internet Security) and the Honeynet project.

[3] Pcap is a packet capture standard supported by both open source and commercial network capture equipment.

creation and release of actuarial threat risk models that incorporate heterogeneous tendencies in variance across multidimensional determinants while maintaining parsimony. I foresee a combination of Heteroscedastic predictors (GARCH/ARIMA etc) coupled with non-parametric survival models. I expect that this will result in a model where the underlying hazard rate (rather than survival time) is a function of the independent variables (covariates). Cox's Proportional Hazard Model with Time-Dependent Covariates would be a starting point, going to non-parametric methods if necessary. The end goal will be to create a framework and possibly a program that can assess data stream based on a number of dependant variables (Threat models, system survival etc) and covariates and return a quantified risk forecast and standard error.

Utility to Department of Homeland Security

When a system fails, it often can fail in numerous ways with several causes for the failure (Crowder 2001). Censored observation management can be considered the principal factor influencing survival analysis. Survival analysis and has developed rigorous procedures and methods effective for the treatment of censored data based on probability theory, asymptotic counting and stochastic process as well as the Martingale central limit theorem. References to the univariate analysis of survival is found in Cox (1972), Cox and Oakes (1984), Fleming and Harrington (1991), Andersen et al (1993), Kalbfleisch and Prentice (1980, 2002), Klein and Moeschberger (2003), Ibrahim et al. (2005), Lawless (1982, 2003), Ma and Krings (2008).

Modeling risk allows it to be measured and controlled.

<u>This work and research follows and continues:</u>

> Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010
>
> Charles Sturt University
>
> http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and (forthcoming)

> Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011
>
> Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in

New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)
Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

Costs, Work, and Schedule

Amount Requested (in dollars):	$2,200,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

• PhD Funding	$480,000
• Supervision	$350,000
• Survey and data Analysis	$230,000
• Research Fellowships (2)	$260,000
• Administration	$120,000
• Costs (Computational Systems)	$660,000
• Support Costs (Coding)	$300,000

BAA Number: BAA 11-02-TTA 01-0127-WP

Offeror Name: W&K INFO DEFENSE RESEARCH LLC

Title Risk Quantification

Date: 07/04/2010

N/A

Operational Capability:

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

Proposed Technical Approach:

The objective of this research is to produce an innovative modeling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

a. constant and homogenous failure rates,

b. binary failure and univariate reliability,

c. censoring of failure data, and

d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

Schedule, Cost, Deliverables, & Contact Info:

Deliverables:

30-40 published papers

3 PhD Thesis' in the field

A commercial model for modeling information risk

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) A Quantitative Analysis into the Economics of Testing Software Bugs, Proceedings of CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls, Proceedings of CISIS 2011, 2011

Corporate Information:

Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253
Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

Proposal White Paper **(Type I)**

BAA number, •	BAA 11-02-TTA 14-0025-WP
Title of proposal;	Software Derivative Markets & Information Security Risk
Name of offeror	W&K INFO DEFENSE RESEARCH LLC
Administrative Contact:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
Technical Contact:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

Amount Requested (in dollars):	$1,200,000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

This project will develop the optimal derivative and risk strategy for software markets. A game theoretic approach to this will be modeled looking at the incentives of the business and programming functions in the organization. Programmers, as optimists (Brooks) hold, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development. This project will deliver frameworks designed to optimize the software development process and to sell the risk using a derivative market place that reflects this risk. The end goal is to remove externalities from the costs of software and incorporate the cost of bad software design into the final cost to the consumer.

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

1.1 Related Work and our contributions

This research will seek to demonstrate that a well-defined software risk derivative market would improve the information exchange for both the software user and vendor removing the oft touted imperfect information state that is said to belie the software industry. In this way, users could have a rational means of accurately judging software risks and costs and as such the vendor could optimally apply their time between delivering features and averting risk in a manner demanded by the end user. After all, it is of little value to increase the cost per unit of software by more than an equal compensating control.

Arora, Telang and Xu asserted that a market based mechanism for software vulnerabilities will necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic pricing game. In the model reported, the players in the market do not report their prices. These players use a model where information is simultaneously distributed to the client of the player and the vendor. The CERT model was touted as being optimal. It relies on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls.

Consequently, the examined "market" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets. As criminal groups and selected security vendors (such as Penetration testers and IDS vendors) have an incentive to gain information secretly , they have an incentive to pay more for unknown vulnerabilities in a closed market. This means that a seller to one of these parties has a reputational incentive to earn more through not releasing information as the individual's reputation will be based on their ability to maintain secrecy.

"Vulnerability disclosure adversely and significantly affects the stock performance of a software vendor. We show that, on average, a software vendor loses around 0.63% of market value on the day of the vulnerability announcement. This translates to a dollar amount of $0.86 billion loss in market value. We also show that markets do not penalize a vendor any more if the vulnerability is discovered by a third party than by the vendor itself."

These results demonstrate that a vendor has an incentive to minimize the vulnerabilities found in their products. If an excessive number of vulnerabilities continue to impact a vendor, their market capitalization suffers as a consequence. This justification offers strong evidence that a vendor does not have an incentive to hide information (as third party vulnerability researchers cause an equal loss in capitalization). It has to be expected that any vulnerability known by the vendor will be uncovered. If the vendor fixes this flaw before release, the cost is minimized and at the limit approaches the cost of testing, (that is a zero incremental cost to that which would be expressed later).

If the vendor discovers a vulnerability in the software they produce, the result is a 'strongly dominated' motive to fix the bug. Hence, any remaining bugs are those that have not been uncovered by the vendor and which are less economical to find (through an increase in testing). It can thus be demonstrated that the vendor knows no more than the user at the point of software release as to the state of bugs in a product.

Testing is far less expensive earlier in the development cycle. Early in the process, the software developer has the greatest returns in testing and bug finding. As the development progresses, the returns are reduced as the process required and the costs associated with finding and correcting software vulnerabilities increases.

The utility is lowest when the software has been shipped to the user. At this point, fixing flaws is an expensive process for both the user and the vendor. This leaves the optimal solution to find as many bugs as possible as early in the development process as is feasible. This contrasts with the increasing costs of finding bugs. This leaves the optimal solution for the vendor based on the discovery of as many bugs as possible as early in the development process as is feasible (as a bug discovered early in the process can cost as much as 10x less than one discovered later) . It does not mean that all bugs or vulnerabilities will be found as the cost of finding additional vulnerabilities quickly exceeds the returns.

The market for lemons requires that the vendor knows the level of flaws better than the user. To many this may seem a common sense outcome, the vendor has access to source code, wrote the program and ran the development process. This is a flawed view as we have demonstrated as it is in the vendor's interest to mitigate vulnerabilities as early as possible. More importantly, the vendor is punished for bugs.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as exist in short sales of stocks). The first contract would be taken by a user and would pay a fixed amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.

This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.

Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.

This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

Utility to Department of Homeland Security

In economic terms, we want to assign liability such that the optimal damage mitigation strategy occurs. The victim will mitigate their damages where no damages for breach apply in respect of the optimal strategy and payoffs. The rule that creates the best incentives for both parties is the doctrine of avoidable consequences (marginal costs liability).

Mitigation of damages is concerned with both the post-breach behaviors of the victim and the actions of the party to minimize the impact of a breach. In a software parlays', this would incur costs to the user of the software in order to adequately secure their systems. This again is a trade-off. Before the breach (through software failures and vulnerabilities that can lead to a violation of a system's security), the user has an obligation to install and maintain the system in a secure state. The user is likely to have the software products of several vendors installed on a single system. Because of this, the interactions of the software selected and installed by the user span the range of multiple sources and no single software vendor can account for all possible combinations and interactions.

Any pre-breach behavior of the vendor and user of software needs to incorporate the capability of the vendors to both minimize the liability attached to their own products, as well as the interactions of other products installed on a system. It is feasible to deploy one of several options that can aid in the minimization of the effects of a breach due to a software problem prior to the discovery of software vulnerabilities, these include:

1. The software vendor can implement protective controls (such as firewalls)
2. The user can install protective controls
3. the vendor can provide accounting and tracking functions

The following steps further facilitate in minimizing the effects of software vulnerabilities:

1. The vendor can employ more people to test software for vulnerabilities
2. The software vendor can add additional controls

Where more time is expended on the provision of software security by the vendor (hiring more testers, more time writing code etc), the cost of the software needs to reflect this additional effort, hence the cost to the consumer increases. This cost is divisible in the case of a widely deployed Operating System (such as Microsoft Windows) where it is easy to distribute the incremental costs across additional users. Smaller vendors (such as small tailored vendors for the Hotel accounting market) do not have this distributional margin and the additional controls could result in a substantial increase in the cost of the program.

Technical Approach

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

This work and research follows and continues that published as:

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010 Charles Sturt University
http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

Costs, Work, and Schedule

Amount Requested (in dollars):	$1,200,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field. The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

• PhD Funding	$360,000
• Supervision	$180,000
• Survey and data Analysis	$220,000
• Administration	$120,000
• Core Systems	$220,000
• Marketing of system and test use	$100,000

BAA Number: BAA 11-02-TTA 01-0127-WP
Offeror Name: W&K INFO DEFENSE RESEARCH LLC
Title Software Derivative Markets & Information Security Risk
BAA 11-02-TTA 14-0025-WP
Date: 07/04/2010

NA

Operational Capability:
The project test, develop and test a combination of insurance and derivative based risk markets for both software security and information risk minimization.

Proposed Technical Approach:
This project will address and provide measures and The analysis will measure the following coding errors:

- Format string errors
- Integer Overflows
- Buffer overruns
- SQL Injection
- Cross-Site scripting
- Race Conditions
- Command Injection.

In addition, market models for selling vulnerabilities will be developed and tested. A first stage vulnerability and risk marketplace will be developed.

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings CISIS 2011 June 8-10th, 2011

Schedule, Cost, Deliverables, & Contact Info:
This project will develop the optimal derivative and risk strategy for software markets. A game theoretic approach to this will be modelled looking at the incentives of the business and programming functions in the organization. Programmers, as optimists (Brooks,) hold,
"the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development. This project will deliver frameworks designed to optimize the software development process and to sell the risk using a derivative market place that reflects this risk. The end goal is to remove externalities from the costs of software and incorporate the cost of bad software design into the final cost to the consumer.

Deliverables:
20-30 published papers
3 PhD Thesis' in the field
A commercial model for software derivatives and insurance markets

Corporate Information:
Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253
Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

Proposal White Paper (Type II)

BAA number, •	BAA 11-02-TTA 05-0155-WP
Title of proposal;	SCADA Isolation
Name of offeror	W&K INFO DEFENSE RESEARCH LLC
Administrative Contact:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
Technical Contact:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

Amount Requested (in dollars):	$1,800,000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.

The Revenant device is an embedded Linux-based appliance with an RFC compliant IPSec and Stateful firewall implementation built into the kernel. It is built using embedded Linux and is completely solid state with no moving parts to fail and no hard drive. It also utilises kernel-based IPSec. Designed as an appliance, this system is modular and highly configurable, requiring a small physical, CPU and memory footprint.

The Revenant appliance platform provides a base set of services and functions as an operating environment for many security conscious network based applications. The Appliance provides built-in IPSec encryption, SSHv2 Secure Remote Management, text based management and power-off safe operation.

Basic Management and upkeep of Revenant

System Life-Cycle comprises:

- Security Patch updates
- System and Application updates
- System health-check and maintenance
- System Security Integrity maintenance

Revenant embodies an imbedded, appliance architecture with a strong bias towards encryption, out-of-band authentication and other network applications.

Two primary products have been designed at this point, with expansion into additional modules planned for the future.

- Revenant Encrypted Private Network Gateway
- The Revenant EPN Gateway provides a platform for performing IPSec encryption in several configurations:
  1) Network-to-Network
  2) Host-to-Network
  3) Host-to-Host
  4) Revenant IDS
- The Revenant application is also capable of providing a platform for an IDS sensor.

The Revenant appliance platform provides a base set of services and functions as an operating environment for many security conscious network based applications. The Appliance provides built-in IPSec encryption, SSHv2 Secure Remote Management, Text based management and power-off safe operation

The Revenant appliance has been built with size, performance and security as primary goals, and as a result of this, the system does not run any network accessible processes except those required by specifically installed modules.

The Revenant platform offers no intrinsic network access paths, and is not accessible on the network unless one of the network modules has been installed. The Revenant system does not load any network accessible functionality except as required by the appliance modules loaded in any specific configuration.

The Revenant Measurement appliance is an "Out-of-Band" strong authentication and connection gateway system. Measurement is an access concentrator, which performs strong authentication of user requests. In a security conscious environment, the Measurement allows an organization to effectively provide wide-ranging access to systems or services through a single, secure access path.

The Revenant appliance is a perfect platform for Measurement services due to the security functions and services built into the base system.

1.1 Related Work and our contributions

This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.

Technical Approach

A PCap module written in R and C that can take direct network feeds (TCP/IP) and report on anomalous traffic (with a learning feature and feedback cycle to minimize error with use) will be developed with the appliance.

<u>This work and research follows and continues that published as:</u>

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010 Charles Sturt University
http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China Charles Sturt University and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and URL:
http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

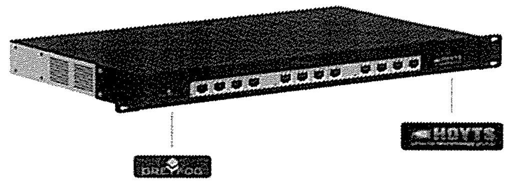
Costs, Work, and Schedule

Amount Requested (in dollars):	$1,800,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for two (2) PhD candidates to aide in the research and investigation of security issues and solution, the creation of software and IDS tools in this field. The period is set to three years which includes the completion of the PhD projects and the creation of the appliance and related open source software.

• PhD Funding	$240,000
• Supervision	$180,000
• Survey and data Analysis	$120,000
• Administration	$120,000
• Core Systems	$220,000
• Marketing of system and test use	$100,000
• Software coding	$340,000
• Electronics and System	$480,000

BAA Number: BAA 11-02-TTA 05-0155-WP
Offeror Name: W&K INFO DEFENSE RESEARCH LLC
Title SCADA Isolation
Date: 07/04/2010



Operational Capability:
The project test, develop and test a set of software and hardware solutions developed to minimize attacks again SCADA systems.

Proposed Technical Approach:
This project will provide a low cost, high availability and security SCADA security solution through:

- System inventory management
- Firewall
- Anti-virus / anti-malware
- Forensic network capture
- IP property protection and extrusion reporting
- Risk quantification
- Advanced traffic filtering and data capture
- The idea to be patented – advanced IDS / honeypot

Schedule, Cost, Deliverables, & Contact Info:
This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.

Deliverables:
5-10 published papers
2 PhD Thesis' in the field
A commercial appliance
A TCPDump filter program

Corporate Information:
Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253
Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

Proposal White Paper	**(Type I)**
<u>BAA number</u>, •	BAA 11-02-TTA 09-0049-WP
<u>Title of proposal;</u>	Risk Quantification
<u>Name of offeror</u>	W&K INFO DEFENSE RESEARCH LLC
<u>Administrative Contact</u>:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
<u>Technical Contact</u>:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

Amount Requested (in dollars):	$2,200,000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

Using empirical evidence, this research aims to investigate and quantify the root cause of security flaws that act as a source of system compromise. Research into the effects of poor system design, market based risk solutions based on derivative instruments and the impact of common system misconfigurations will be incorporated into multivariate survival models. This research incorporates the economic impact of various decisions as a means of determining the optimal distribution of costs and liability when applied to information security and in particular when assigning costs in computer system security and reliability engineering.

The objective of this research is to produce an innovative modelling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

   a. constant and homogenous failure rates,
   b. binary failure and univariate reliability,
   c. censoring of failure data, and
   d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

To do this, it is necessary to recognise that information security is a risk function (Anderson, Longley & Kwok, 1994). Paying for too much security can be more damaging in economic terms than not buying enough. This leads to decisions about where the optimal expenditure on damage prevention should lie. This research will investigate who should be responsible for the security failures that are affecting the economy and society and how can this be maximized in order to minimize negative externalities (Cohen, 1976). The conclusions will be presented using an empirical study of software hazard rates and audit failures along with the question of how to enforce liability in a global economy.

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

The introduction of Game Theory and Behavioural Economics (Anderson, 2001; Anderson, & Moore, 2006; Varian, 2004) have created a foundation for the rationalisation of information security processes which lead to improved allocation of economic resources. The optimal distribution of economic resources across risk allocations in information system can only lead to

a combination of more secure systems for a lower overall cost. This research will incorporate the game theoretic multi-player decision problem. Agents in the model will be deemed to be rational with well-defined preferences, include the ability to reason strategically using their knowledge and belief of other players and to act according to a combination of both economic "*first thought*" and deep strategic thinking (Nissan, et. al., 2007). Solutions to these models will be sought through a combination of the following game devices:

- Equilibrium: evolutive (steady state) games
- Heterogeneous sequential games
- Rationalisability: deductive reasoning

The models will detail the existence of strictly dominating games where these exist in information security practices and propose methods to improve these models. Existing information security practices in existing organisations will be classified into the following game types:

- Non-cooperative vs. cooperative game
- Strategic vs. extensive game
- Perfect vs. imperfect information

Bounded rationality, behavioural game aspects and other feedback effects will be investigated (Nissan, et. al., 2007). Social capital based on fairness and reciprocity will be defined as it applies to the economically efficient application of risk processes associated with Information systems. Contract Theory will be used to explain the creation of agreements and "*contracts*" in the presence of information asymmetry. This is approached through the combination of adverse selection, moral hazards and the "*signalling game*". In this, adverse selection is defined as the "*Principal not having been informed of the other agent's private information ex-ante*" such as in George Akerlof's "*Market for lemons*" (1970). This application of game theory has been asserted to explain many aspects of the software industries predisposition to create insecure software (Anderson, 2001). Arora, Telang and Xu (2004) asserted that a market-based mechanism for software vulnerabilities would necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic *pricing game*. In the model reported, the players in the market do not report their prices[1]. These players use a model where information is distributed simultaneously to the client of the player and the vendor. The CERT model was touted as being the most favourable solution. The research will demonstrate that the examined "*market*" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets that rely on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls. It is to be demonstrated that there are flaws with this approach that can be solved through the creation of a security and risk derivative market for software. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs (Bacon et. al. 2009).

1.2 Our contribution and Technical Approach

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing security vulnerabilities. The goal of this research project is to create a series of quantitative models for information security. Mathematical modelling techniques that

[1] E.g., iDefense Ltd. and other similar providers have a semi-closed market with limited information exchange.

can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modelling,
- Behavioural Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modelling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

This data will be coupled with hazard models created and validated using Honeynets (e.g. Project Honeynet), reporting sites such as the Internet Storm Centre and iDefence. The combination of this information will provide the framework for a truly quantitative security risk framework[2]. At present, the DShield storm centre receives logging from over 600,000 organisations. This represents a larger quantity of data than is used for actuarial data in the home insurance industry. The problem being that this information is not collated or analysed in any quantitatively sound manner. This research will model survival times for types of applications using the body of research into quantitative code analysis for risk. The research will create a series of models (such as those used within mechanical engineering, material science etc) for Information Risk.

Some of the methods that are planned testing in the creation of the risk framework will include:

- Random forest clustering,
- K-means analysis,
- Other classification algorithms, and
- Network associative maps in text analysis forensic work.

The correlation of reference data (such as IP and functional analysis data) between C&C (Command and Control) systems used in "*botnets*" is one aspect of this research. Starting from the outside (the cloud and perimeter) and working inwards to the network, the risk model would start by assessing external threats and move into internal threat sources, becoming gradually become more and more granular as one moves from network to individual hosts and finally to people (user behaviour (Varian, 2004)) and application modelling (Guo, Jarrow, & Zeng, 2005). The eventual result will be the creation of a model that can incorporate the type of organisation, size, location, application, systems used, and the user awareness levels to create a truly quantitative risk model. This would be reported with SE (standard error) and confidence level rather than a point estimate. Code to import data from hosts and networks, using raw "*pcap traces*"[3] will be developed such that system statistics and other data can be collated into a standardised format. This code will be developed in "R" and "C++". This will enable the

[2] Support has been sought and received from SANS (including DShield), CIS (Centre for Internet Security) and the Honeynet project.

[3] Pcap is a packet capture standard supported by both open source and commercial network capture equipment.

creation and release of actuarial threat risk models that incorporate heterogeneous tendencies in variance across multidimensional determinants while maintaining parsimony. I foresee a combination of Heteroscedastic predictors (GARCH/ARIMA etc) coupled with non-parametric survival models. I expect that this will result in a model where the underlying hazard rate (rather than survival time) is a function of the independent variables (covariates). Cox's Proportional Hazard Model with Time-Dependent Covariates would be a starting point, going to non-parametric methods if necessary. The end goal will be to create a framework and possibly a program that can assess data stream based on a number of dependant variables (Threat models, system survival etc) and covariates and return a quantified risk forecast and standard error.

Utility to Department of Homeland Security

When a system fails, it often can fail in numerous ways with several causes for the failure (Crowder 2001). Censored observation management can be considered the principal factor influencing survival analysis. Survival analysis and has developed rigorous procedures and methods effective for the treatment of censored data based on probability theory, asymptotic counting and stochastic process as well as the Martingale central limit theorem. References to the univariate analysis of survival is found in Cox (1972), Cox and Oakes (1984), Fleming and Harrington (1991), Andersen et al (1993), Kalbfleisch and Prentice (1980, 2002), Klein and Moeschberger (2003), Ibrahim et al. (2005), Lawless (1982, 2003), Ma and Krings (2008).

Modeling risk allows it to be measured and controlled.

This work and research follows and continues:

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in

New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)
Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

Costs, Work, and Schedule

Amount Requested (in dollars):	$2,200,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

• PhD Funding	$480,000
• Supervision	$350,000
• Survey and data Analysis	$230,000
• Research Fellowships (2)	$260,000
• Administration	$120,000
• Costs (Computational Systems)	$660,000
• Support Costs (Coding)	$300,000

BAA Number: BAA 11-02-TTA 01-0127-WP

Offeror Name: W&K INFO DEFENSE RESEARCH LLC

Title Risk Quantification

Date: 07/04/2010

N/A

Operational Capability:

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

Proposed Technical Approach:

The objective of this research is to produce an innovative modeling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

a. constant and homogenous failure rates,

b. binary failure and univariate reliability,

c. censoring of failure data, and

d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

Schedule, Cost, Deliverables, & Contact Info:

Deliverables:

30-40 published papers

3 PhD Thesis' in the field

A commercial model for modeling information risk

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) A Quantitative Analysis into the Economics of Testing Software Bugs, Proceedings of CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls, Proceedings of CISIS 2011, 2011

Corporate Information:

Dave Kleiman

W&K INFO DEFENSE RESEARCH LLC

4371 Norhtlake Blvd #314

Palm Beach

FL 33410 - 6253

Phone: 5613108801

Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

Proposal White Paper	**(Type I)**
BAA number, •	BAA 11-02-TTA 01-0127-WP
Title of proposal;	Software Assurance through Economic Measures
Name of offeror	W&K INFO DEFENSE RESEARCH LLC
Administrative Contact:	Dave Kleiman
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	NA
TIN:	274997114
Technical Contact:	Craig Wright
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	+61 2 4362 1512
Fax:	NA
TIN:	274997114

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and an Australian Research Company.

Amount Requested (in dollars):	$650000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business

Executive Summary

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

1.1 Related Work

Other studies of coding processes and reliability have been conducted over the last few decades. The majority of these have been based either on studies of large systems and mainframe based operations or have analyzed software vendors. In the few cases where coding practices within individual organization have been quantitatively analyzed, the organizations have been nearly always large telecommunications firms or have focused on SCADA and other critical system providers.

Whilst these results are extremely valuable, they fail to reflect the state of affairs within the vast majority of organizations. With far more small to medium businesses coupled with comparatively few large organizations with highly focused and dedicated large scale development teams (as can be found in any software vendor), an analysis of in-house practice is critical to both security and the economics of in-house coding.

As the Internet becomes all persuasive, internal coding functions are only likely to become more prevalent and hence more crucial to the security of the organization.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as exist in short sales of stocks). The first contract would be taken by a user and would pay a fixed amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.

This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.

Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.

This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

Utility to Department of Homeland Security

The game theoretic approach to this can be modeled looking at the incentives of the business and programming functions in the organization. Programmers are optimists. As Brooks noted, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development.

Technical Approach

Just as car dealers buff the exterior and detail the upholstery of a used car, neglecting the work that should be done on the engine, software vendors add features. Most users are unlikely to use even a small fraction of these features, yet they buy the product that offers more features over the more secure product with fewer features. The issue here is that users buy the features over security. This is a less expensive option for the vendor to implement and provide.

The creation of a security and risk derivative should change this. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs. This would most likely lead to product differentiation (as occurred in the past with Windows 95/Windows NT). Those businesses who wish to pay for security could receive it. Those wanting features would get what they asked for.

It is argued that software developers characteristically do not correct all the security vulnerabilities and that known ones remain in the product after release. Whether this is due to a lack of resources or other reasons, this is unlikely to be the norm and would be rectified by the market. The cost of vendors in share price and reputational losses exceed the perceived gains from technical reasons where the fix might break existing applications. The application is already broken in the instance of a security vulnerability.

Users could still run older versions of software and have few, if any, bugs. The issue is that they would also gain no new features. It is clear that users want features. They could also choose to use only secure software, but the costs of doing so far outweigh the benefits and do not provide a guarantee against the security of a system being compromised. As such, the enforced legislation of security standards against software vendors is detrimental. A better approach would be to allow an open market based system where vendors can operate in reputational and derivative markets.

At the end of any analysis, security is a risk function and what is most important is not the creation of perfectly security systems, but the correct allocation of scarce resources. Systems need to be created that allow the end user to determine their own acceptable level of risk based on good information.

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

<u>This work and research follows and continues that published as:</u>

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China

Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Personnel and Performer Qualifications and Experience

Craig S Wright (Full CV too long and is available in request)

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

Dave Kleiman (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

Bob Radvanovsky, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and Implication", ISBN 1616928050 and 9781616928056, Information Science Publishing, July 2010.

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

"Challenges Faced by the SCADASEC Mailing List", Protecting Canada's Critical Infrastructure 2010 Control Systems Security Workshop, sponsored by Royal Canadian Mounted Police (Ontario Technological Crime), Public Safety Canada and Emergency Management Ontario (Critical Infrastructure Assurance Program), Wednesday April 14, 2010 and Thursday, April 15, 2010.
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
Author of "Critical Infrastructure: Homeland Security and Emergency Preparedness", Second Edition, ISBN 1420095277 and 9781420095272, Taylor & Francis CRC Press, December 2009.
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
Contributor (introduction speaker) of "The Year in Homeland Security", 2008/2009 Edition (Charles Oldham, editor director), Faircount Media Group.
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
Author (co-author) of "Transportation Systems Security", ISBN 1420063782 and 9781420063783, Taylor and Francis CRC Press, May 2008.
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

Commercialization Capabilities and Plan

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

Costs, Work, and Schedule

Amount Requested (in dollars):	$650,000.00
Duration:	36 months

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

• PhD Funding	$240,000
• Supervision	$180,000
• Survey and data Analysis	$230,000

BAA Number: BAA 11-02-TTA 01-0127-WP
Offeror Name: W&K INFO DEFENSE RESEARCH LLC
Title Software Assurance through Economic Measures
Date: 07/04/2010

N/A

Operational Capability:
The project will analyze a sample of at least 1,000 coding projects using existing static analysis tools, manual code review and related techniques. Where these methods are lacking, proposals and methods to integrate existing methods and to fill the gaps left will be created.

Proposed Technical Approach:
This project will address and provide measures and The analysis will measure the following coding errors:

- Format string errors
- Integer Overflows
- Buffer overruns
- SQL Injection
- Cross-Site scripting
- Race Conditions
- Command Injection.

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Schedule, Cost, Deliverables, & Contact Info:
Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.

Deliverables:
20-30 published papers
3 PhD Thesis' in the field
A commercial model for software derivatives and insurance markets

A means to measure and predict the following coding errors is being developed
Format string errors
Integer Overflows
Buffer overruns
SQL Injection
Cross-Site scripting
Race Conditions
Command Injection.

Corporate Information:
Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253

Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature: Craig S Wright

S&T Directorate BAA Cover Sheet A

Proposal Does Not Contain Proprietary Information

Proposal Number:	BAA 11-02-TTA 14-0025-WP
Topic:	TTA 14 - Software Assurance MarketPlace (SWAMP)
Proposal Title:	Software Derivative Markets & Information Security Risk
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	
TIN:	274997114
DUNS + 4:	null -
CAGE Code:	
SIC:	
FICE:	
Proposal Contains Proprietary Information:	No
Amount Requested (*in dollars*):	$1200000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less Small Business

M

This is the annexure marked with the letter M referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT ~~sworn~~/affirmed/~~declared~~ before me at Sydney on the 4th day of November 2013

~~One page only~~
Page 1 of 6 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

S&T Directorate BAA Cover Sheet A

Proposal Does Not Contain Proprietary Information

Proposal Number:	**BAA 11-02-TTA 09-0049-WP**
Topic:	**TTA 09 - Cyber Economics**
Proposal Title:	**Risk Quantification**
Company Name:	**W&K INFO DEFENSE RESEARCH LLC**
Mailing Address (Line 1):	**4371 Norhtlake Blvd #314**
Mailing Address (Line 2):	
City:	**Palm Beach**
State & Zip Code:	**FL 33410 - 6253**
Phone:	**5613108801**
Fax:	
TIN:	**274997114**
DUNS + 4:	**null -**
CAGE Code:	
SIC:	
FICE:	
Proposal Contains Proprietary Information:	**No**
Amount Requested (*in dollars*):	**$2200000.00**
Duration:	**36 months**
Requested Starting Date:	**07/04/2011**
Business Type:	**Small Business** **Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less**

S&T Directorate BAA Cover Sheet A

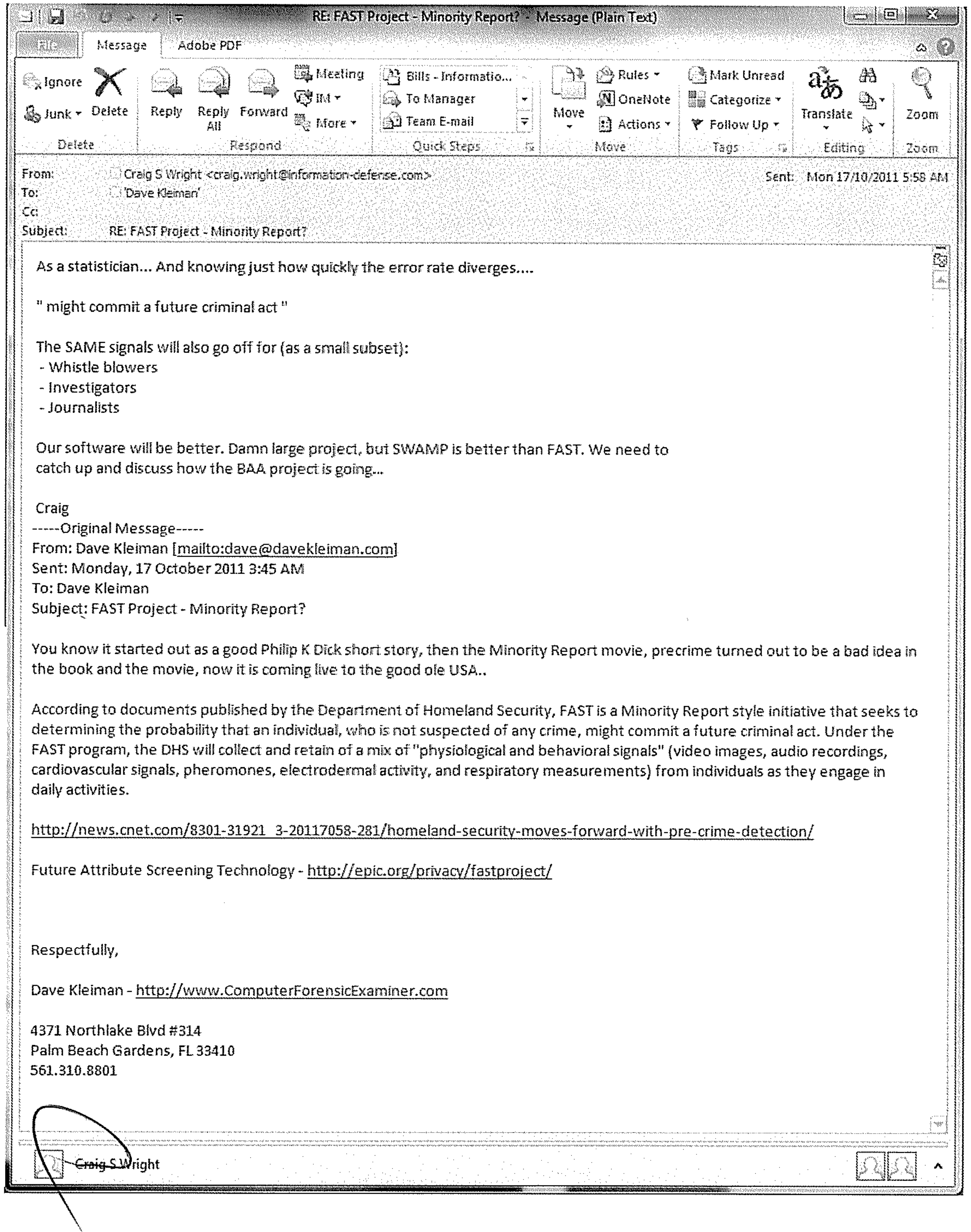
Proposal Does Not Contain Proprietary Information

Proposal Number:	BAA 11-02-TTA 05-0155-WP
Topic:	TTA 05 - Secure, Resilient Systems and Networks
Proposal Title:	SCADA Isolation
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	
TIN:	274997114
DUNS + 4:	null -
CAGE Code:	
SIC:	
FICE:	
Proposal Contains Proprietary Information:	No
Amount Requested (*in dollars*):	$1800000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less Small Business

S&T Directorate BAA Cover Sheet A

Proposal Does Not Contain Proprietary Information

Proposal Number:	BAA 11-02-TTA 01-0127-WP
Topic:	TTA 01 - Software Assurance
Proposal Title:	Software Assurance through Economic Measures
Company Name:	W&K INFO DEFENSE RESEARCH LLC
Mailing Address (Line 1):	4371 Norhtlake Blvd #314
Mailing Address (Line 2):	
City:	Palm Beach
State & Zip Code:	FL 33410 - 6253
Phone:	5613108801
Fax:	
TIN:	274997114
DUNS + 4:	null -
CAGE Code:	
SIC:	
FICE:	
Proposal Contains Proprietary Information:	No
Amount Requested (*in dollars*):	$650000.00
Duration:	36 months
Requested Starting Date:	07/04/2011
Business Type:	Small Business Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less



From: Craig S Wright <craig.wright@information-defense.com>
To: 'Dave Kleiman'
Cc:
Subject: RE: FAST Project - Minority Report?
Sent: Mon 17/10/2011 5:58 AM

As a statistician... And knowing just how quickly the error rate diverges....

" might commit a future criminal act "

The SAME signals will also go off for (as a small subset):
- Whistle blowers
- Investigators
- Journalists

Our software will be better. Damn large project, but SWAMP is better than FAST. We need to catch up and discuss how the BAA project is going...

Craig
-----Original Message-----
From: Dave Kleiman [mailto:dave@davekleiman.com]
Sent: Monday, 17 October 2011 3:45 AM
To: Dave Kleiman
Subject: FAST Project - Minority Report?

You know it started out as a good Philip K Dick short story, then the Minority Report movie, precrime turned out to be a bad idea in the book and the movie, now it is coming live to the good ole USA..

According to documents published by the Department of Homeland Security, FAST is a Minority Report style initiative that seeks to determining the probability that an individual, who is not suspected of any crime, might commit a future criminal act. Under the FAST program, the DHS will collect and retain of a mix of "physiological and behavioral signals" (video images, audio recordings, cardiovascular signals, pheromones, electrodermal activity, and respiratory measurements) from individuals as they engage in daily activities.

http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/

Future Attribute Screening Technology - http://epic.org/privacy/fastproject/

Respectfully,

Dave Kleiman - http://www.ComputerForensicExaminer.com

4371 Northlake Blvd #314
Palm Beach Gardens, FL 33410
561.310.8801

Craig S Wright

This is the annexure marked with the letter L referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig SWRIGHT
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

N

Integyrs

The following is a response to the request by the ATO, ref. 1011685995901.

Enterprise

1. Income is on hold at present. The ATO has been auditing and reviewing the company following an initial question as to the allocation of GST that lead to a zero amount in payment overall.
    a. Income was based on an arrangement with a large multi-national form for the export of software and mathematical algorithms.
    b. The company plans to raise money and sell its IP and software.
    c. To do this, it needs to get past the audit phase.
    d. No income is expected to when the ATO allows us to actually carry on a business.
    e. Basically, we are conducting research and developing capital in the hope that one day the auditing process will actually provide some feedback and we can go to market. This was in progress before the ATO started calling clients and placed this on hold.
2. Australia
3. 24x7
4. International
    a. We have published malware papers and processes (peer reviewed)
    b. We have published statistical libraries
    c. These can be sold as .Net framework libraries. Large companies such as Microsoft, MacAfee and CA have interest in the IP, but we need to have cleared the audit before we can sell this.
5. All contract – see 2010 tax return.
    a. Income is on hold to when we can sell
    b. Sales will not start until the audit is complete
    c. Sales had started before the ATO started contacting clients who then placed holds on the sales.
6. All work is currently completed by directors and contractors.

This is the annexure marked with the letter N referred to in the Affidavit /
Af~~firmation / Statutory Decl~~aration of Craig S WRIGHT
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2017

~~One page only~~
Page 1 of 10 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

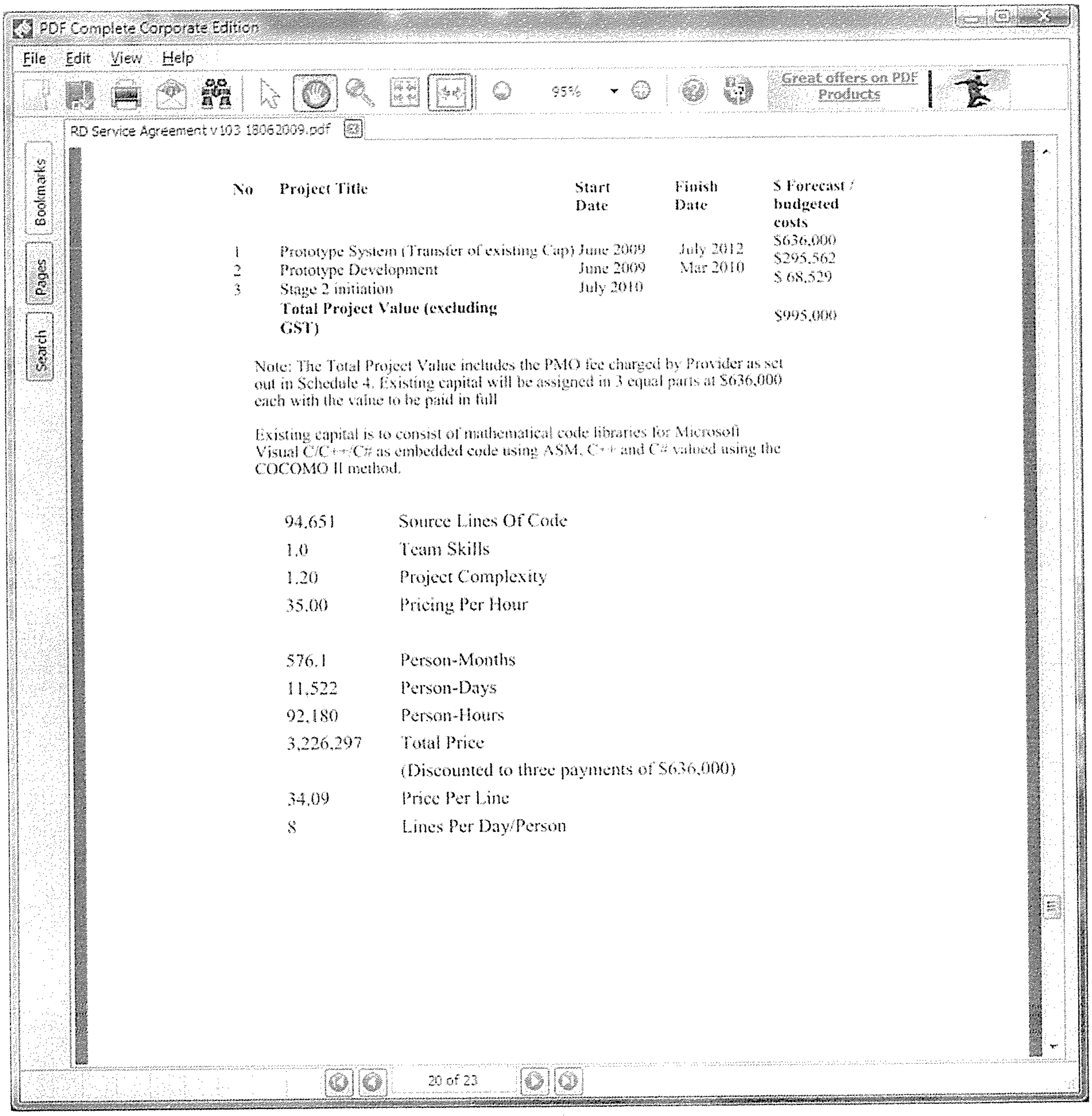
Supplies

1. Data warehousing
    a. Contracting
    b. Rental of office space
    c. Computer systems
    d. Software
    e. Previously Existing IP
2. See folders.
    a. Q4 2010 has not been completed and hence is not included in this.

Capital Acquisitions

Plant leasing and core tech.

1. Transfer of developed code into the company.
    a. COCOMO used to cost technology.
2. Leasing of systems for the following 12 months.


PDF Complete Corporate Edition
File Edit View Help
95%
Great offers on PDF Products
RD Service Agreement v103 18062009.pdf
Bookmarks
Pages
Search
20 of 23

No	Project Title	Start Date	Finish Date	$ Forecast / budgeted costs
1	Prototype System (Transfer of existing Cap)	June 2009	July 2012	$636,000
2	Prototype Development	June 2009	Mar 2010	$295,562
3	Stage 2 initiation	July 2010		$ 68,529
	Total Project Value (excluding GST)			$995,000

Note: The Total Project Value includes the PMO fee charged by Provider as set out in Schedule 4. Existing capital will be assigned in 3 equal parts at $636,000 each with the value to be paid in full

Existing capital is to consist of mathematical code libraries for Microsoft Visual C/C++/C# as embedded code using ASM, C++ and C# valued using the COCOMO II method.

94,651	Source Lines Of Code
1.0	Team Skills
1.20	Project Complexity
35.00	Pricing Per Hour
576.1	Person-Months
11,522	Person-Days
92,180	Person-Hours
3,226,297	Total Price
	(Discounted to three payments of $636,000)
34.09	Price Per Line
8	Lines Per Day/Person

The IP has been deducted at a rate of 3 years as this is the perceived life of the IP before patient. This is at $666,666 as 1/3rd of the total costs to date.

Evidence

See contract – copy on disk

Capital Value

Direct costs plus IP

Valuation

CoCOMO II based methodology plus direct costs.

Use in the Enterprise

The systems and equipment are used directly in the research and the development of solutions that will be offered for international sale.

This Research is directly linked to a PhD candidacy at Charles Sturt University and is related to a CRiCS research study.

The PhD proposal and associated research papers are available on request.

Other Acquisitions

Non-capital acquisitions for the period 01/01/2010 to 31/21/2010 as per purchase schedule. This includes Carbon credits (to offset computers using electricity) and sundry expenses.

2010 Income Tax Return

Invoices – see disk

Payments – see disk

Loans

– see disk

The following loan contracts have been attached (as prepared by Michie Shehadie and Co and registered).

Loan from Lynn Wright

Loan from Craig Wright

Other Loans (Visa and sundry expenses)

Current Assets and Liabilities

See MYOB File on disk.

This includes depreciating assets.

These assets are used in the research projects and are key to the development of product.

Intellectual Property

Acquisition – how

R& D intellectual property sold by Craig Wright to Integyrs Pty Ltd

- You have valued the market value of your intellectual property as $2,246,000 (data from your BAS (Craig Wright) for the tax periods July – Dec 2009) which you sold to two of your companies where you are the Director.
- You have to provide documents to substantiate that you have incurred these costs during the course of your research and development of your intellectual property.
- Please provide substantiation of the above costs by providing the tax invoices with full details of the supplier, date, description and the amounts stated for the purchases.

Sale of Capital Assets to Integyrs Pty Ltd 95 137 033 535

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

Contracts created by Mitchie Shehadie and Co.

I have attached these documents on the disk and with each sale contract. This includes a schedule as what IP was transferred.

I have attached a spreadsheet with the breakdowns of loans by Lynn Wright for total for a 7% interest rate. The total comes to $815,803.61 as of 01 Jul 2009.

The amounts are covered as follows in the spreadsheet under the following headers:

<u>Conferences and Travel</u>

Lynn paid monies for my attendance at conferences

These where for my business and education (e.g. SANS)

<u>Monthly Contributions</u>

Lynn helped me pay the loans used for the legal costs.

As per the attached information in the attached email, as per 'Farrugia v The Official Receiver (1982) 43 ALR 700' The Doctrine of Exoneration is used in the allocation of these when applied to real property. The loans where for the direct purpose of Integyrs and Research at Lynn's detriment. These amounts are monies she paid towards the loan each month and are hence loaned to the company.

<u>Debt - Purchased contract</u>

DeMorgan Pty Ltd had a contract for $105,000 pa in payments to Lynn on sale.

I purchased this in order to by the business of DeMorgan and start DeMorgan Information Security Systems P/L and this contract and the IP associated with it was transferred into Integyrs.

Valuation

CoCOMO II for software

Cost basis and transfer for prior assets.

Assets and shares moved from prior companies set as per court order issued by NSW Supreme court.

Supplier Agreements

Sale of Capital Assets to Integyrs Pty Ltd

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

$1,100,000

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

$1,100,000

Associated IP as maintined following – Liquidation of DeMorgan Information Security Systems Pty Ltd and kept due to unpaid debt.

Shares and debt	$ 2,178,000

As determined by NSW Supreme Court.

Losses – Depreciation of capital Assets (Write-off)

Old Computer Equipment	$22287

Total Gains	$2,235,000
Total Losses	$34,713

Bank Statements

See folder – 1 statement.

AusIndustry

Yes, Integyrs is registered with AusIndustry.

R2010976