OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Mr. James Tucker
Mr. Shane Witnov
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

MAY 14 [illegible]

Reference: DF-2010-00004

Dear Mr. Tucker and Mr. Witnov:

This responds to your 6 October 2009 letter addressed to the Director, Information Management Office, Office of the Director of National Intelligence. You requested, under the Freedom of Information Act (FOIA), **"copies of all records, including electronic records, concerning use of social-networking websites (including but not limited to Facebook, MySpace, Twitter, Flickr, and other online social media) for investigative (criminal or otherwise) or data gathering purposes created since January 2003."**

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. ODNI conducted a search and located ten documents which are responsive to your request. Of those, two documents are being withheld in full pursuant to FOIA Exemption 5, 5 U.S.C. § 552 (b)(5) which protects certain inter- and intra-agency communications protected by the deliberative process privilege.

In addition, five documents are being released with redactions made pursuant to FOIA Exemptions 2 and 6, 5 U.S.C. § 552 (b)(2) and (b)(6). Exemption 2 protects information that is strictly administrative in nature. Exemption 6 protects information which if released would constitute a clearly unwarranted invasion of personal privacy. The three remaining documents are provided with no redactions.

Although this case is currently in litigation, I am required to notify you that you have the right to appeal our decision. Should you choose to do so, you may appeal, in writing to:

Office of the Director of National Intelligence
Information Management Office
Washington, DC 20511

Sincerely,

John F. Hackett
Director, Information Management Office

Informed Consent to Participate in Research

A research project is being conducted by The Office of the Director of National Intelligence, Special Security Center to evaluate the use of available information technology and databases to expedite investigative and adjudicative processes. The federal government is working to improve the personnel security clearance process and your participation will assist in this action. This form requests you, as an applicant for federal employment and/or program access, to consent to the federal agency conducting this research by accessing various open source and publicly accessible information about you.

The information requested below is protected by the Privacy Act of 1974, 5 U.S.C. § 552a. The authority to request it is the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act. The information you provide will not be used for any purpose other than this research project. You are not required to provide this information or to participate in this research. Your Social Security Number, if provided, will be used to conduct wider research of open source information than would be possible otherwise. Refusal to participate will in no way affect determination of your suitability or eligibility for a national security position. To protect your privacy, no information collected in the course of this research will be stored or maintained by individual name; rather, the purpose is to collect statistical data for trend analysis.

Your consent is valid for 1 (one) year from the date signed or upon the termination of your affiliation with the Federal Government, whichever is sooner.

If you have questions regarding this study you may contact [redacted]

b2
b6

If you agree to voluntarily participate in this research as described, please indicate your agreement by signing below

Full name *(Type or print legibly)*

Signature *(Sign in Ink)* Date signed *(mm/dd/yyyy)*

Other names used

Date of Birth Social Security Number

Current street address Apt. # City *(Country)* State Zip Code

Home telephone number

January 25, 2008

Web Scrub Validation

Concept of Operations

The Nature of the Project

This project is a preliminary survey. It is intended to help determine whether there is any merit in including in background investigations for access to classified information reviews of individuals' unprotected web presence. By "unprotected web presence," we mean those things posted on the Internet that are openly available to anyone with a browser; we do *not* mean anything whose access is limited in any way, such as by being password protected. The personnel security process includes examination of a person's behavior both on the job (through, for example, employment histories and supervisor and co-worker interviews) and off duty (through, for example, credit checks, criminal history checks, and neighborhood interviews). A person's unprotected web presence may be relevant to both, but in particular to the latter.

This survey is an attempt to determine what *types* of information may be available. We were made aware through our contact with Corporate Risk Interational that it is not uncommon for them to provide web-scrubbing services for clients in the financial sector as part of background investigations. This has become an area of interest as individuals increasingly are posting personal information on publicly accessable websites, in particular the popular social networking sites. This is not a detailed study. It will not be used to suggest modifications to existing investigative standards. No information collected will be used in the adjudication process, because at this time we have no sense of the validity or reliability of any such information. It is simply an initial approach to increase our knowledge and awareness of what types of information are posted in these sites so that educated decisions can be made regarding any future research.

The project is consistent with the Intelligence Reform and Terrorism Prevention Act of 2004's requirement for "evaluation of use of available technology in clearance investigations and adjudications."

Step-by-Step Procedures

1. We will contract through SPAWAR Systems Center, Charleston, SC, with Corporate Risk International, a company we became aware of when surveying employee screening practices in the financial and gaming industries. Corporate Risk International conducts the sorts of searches relevant to this survey for its commercial clients. We chose to work through SPAWAR because our existing relationship with them facilitates the letting of such contracts.
2. Working with not more than three IC agencies, we will identify at random applicants who will be asked to participate in the survey.
3. Each applicant agreeing to participate will sign a separate consent form. The survey requires 400 participants.

4. We will prepare a MIPR to SPAWAR, who will perform program management.
5. Agencies will provide basic identifying data through SPAWAR to Corporate Risk International.
6. Corporate Risk International will conduct Internet searches based on the information provided.
7. Corporate Risk International will prepare a report of its findings. The report will include *no* identifying information. It will contain the *kinds* and *frequencies* of information discovered in its searches. Corporate Risk International itself will retain no record that it conducted a search on a specific person or of the results of that search.
8. The DNI Special Security Center will analyze the anonymized report and make an assessment of the kinds of and quantity of information provided and of its potential relevance to national security adjudications. It will assess whether the results of the survey justify additional work.
9. *If* the results of the survey are suggestive and justify further work, the Special Security Center will commence design of a formal research project which will include thorough legal vetting.

OFFICE of the DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

STATEMENT OF WORK

Open Source Research Project

Submitted:

June 19, 2008

SPAWAR

Systems Center
Charleston

Prepared By:

Space and Naval Warfare Systems Center
P.O. Box 190022
North Charleston, SC 29419-9002

STATEMENT OF WORK

START DATE: Upon award
COMPLETION DATE: 3 months after award
SHORT TITLE: ODNI Open Source Research Project

1. PLACE(S) OF PERFORMANCE

a. SPAWAR Designated Facilities
b. Corporate Risk International, CRI
c. MC Dean, Chantilly, VA
d. ODNI Special Security Center (SSC)

2. REFERENCES

The latest revision of the following guidance documents forms a part of this SOW. In cases where documentation conflicts, for clarification, the SPAWAR Project Manager shall be notified, in writing, and shall make the final determination.

a. Standard Form 86 – Questionnaire for National Security Positions
b. Privacy Act – 5 USC 552a(b)
c. Latest ODNI Open Source Project Privacy Response

3. SPECIFICATIONS

NONE

4. SECURITY REQUIREMENTS

a. Maximum required clearance is SECRET.
b. All visit requests shall be forwarded to the place of performance via the SPAWAR Systems Center Charleston Technical Point of Contact for certification of the "Need-To-Know". All requests shall contain the information required by the NISPOM and shall not exceed the completion date of this order. The DD-254 of the basic contract applies.
c. Government issued personal information shall be protected as required by privacy act and destroyed at the completion of this task. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction. Inappropriate disclosure, lost, stole, or compromised Privacy Act data shall be reported to the SPAWAR PE immediately. Deliverables that include Privacy Act data shall be marked as "For Official Use Only - Privacy Act Data" at the top and bottom of each page.

5. COR DESIGNATION

b6

The COR for this delivery order is [redacted] who can be reached at (843) 218-4439 or e-mail: [redacted] The SPAWAR project engineer that has a specific interest in this work is [redacted] who can be reached at (843) 218-4080.

6. DESCRIPTION OF WORK

<u>Project Background</u>: The Office of the Director of National Intelligence (ODNI) Special Security Center (SSC) Research program coordinates, conducts and oversees research in the area of personnel security to include issues relating to investigations, adjudications and polygraph. Research is conducted at high level and depending on the area of research with participation with Government and non-Government research organizations.

The Intelligence Reform and Terrorism Prevention Act of 2005 mandates the "use of available technology in clearance investigations and adjudications". In support of the Intelligence Reform and Terrorism Prevention Act of 2005, the Director of National Intelligence considers personnel security a high priority and it is a major objective of his "100 Day Plan for Integration and Collaboration" to Modernize Business Practices and apply best practices to the personnel security arena. In recent years, the expanded use of the internet and the upsurge in social networking websites have added new concerns to the personnel security process and a new dimension to investigating a person's background and behavior.

<u>Project Overview:</u> The scope and nature of this study is "fact finding" to determine if meaningful personal information may be obtained from open source websites to determine if social behavior, often referred to as social networking in the cyber world, may reflect personal information that may be deemed as unprofessional, unethical or unacceptable to an employer (government agency). The study will also focus on the content of information that may be posted on open websites or "chat rooms" to determine if sensitive or classified information has been posted or transmitted via an unauthorized communication source.

This SOW covers the effort involved to perform such a study as described above and provide a report based on the findings. Tasks include the following:

a. Project Management

b. Statistical Study

6.1 Task A – Project Management

Task Description: The Contractor shall develop documentation outlining the baseline project approach to the ODNI SSC Program Manager within ten working days after funds are received. Within the baseline project approach, the contractor shall articulate the data/information required from the sponsor in order to complete the project. The POA&M shall include deliverables to be provided as specified in this SOW and must show completion of the tasking contained, to include all review periods for the documents produced. The Contractor shall update this schedule monthly using an Actual versus Baseline tracking method.

6.1.1 Deliverable Product: The deliverable products for this task shall consist of the following:

a. Plan of Action and Milestones (Microsoft Project) – Baseline Submission
b. Plan of Action and Milestones (Microsoft Project) – Monthly Submissions

6.1.2 Task Schedule: The Contractor shall receive approval of the POA&M from the Government prior to beginning work on the other tasks in this SOW. The Government will notify the Contractor within three (3) working days with approval or changes to the POA&M. An updated version of the POA&M shall be delivered with each monthly status report submission using an Actual versus Baseline tracking basis and provide the SPAWAR Project Manager (PM) with an electronic copy of the updated POA&M. The updated POA&M shall identify tasks, dependencies, actual start dates, durations, actual finish date, slippage, percent complete, and resources.

6.2 Task B – Statistical Study

Task Description: The primary goal of the "study" is to determine if social networking websites provide relevant information regarding the personal conduct of an individual that could reflect lack of professional or unethical behavior, potential criminal or statutory misbehavior, or the unauthorized publication of sensitive or even classified U.S. Government information. Based on the study a statistical analysis will be conducted to determine if the information collected may offer new methodologies for collecting and monitoring the behavior of employees that goes beyond the traditional inquiries conducted during the background and re-investigative process. The final report will provide conclusions and a next step as appropriate.

SPAWAR will provide the contractor with biographical information on 400 individuals limited to name, SSN, Place of Birth, Date of Birth for the test cases included in this study. Test cases will be selected pseudo-randomly from the Intelligence Community. Some specific common name test cases (i.e. Joseph Smith) may be selected to evaluate. All Government issued test cases issued for conducting due diligence inquiries via social networking websites will have completed and signed a Standard Form 86 (Questionnaire for National Security Positions), and have a completed Single Scope Background Investigation. The investigation will cover, at a minimum, Facebook, MySpace, and U-Tube web logs or "blogs" that may be appropriate to referenced test cases. 400 test cases will be provided to the contractor to perform the above investigations on. A list of the databases that must be searched include the following:

1. Global Internet Search
2. Internet "Blog" Websites
3. Internet Social Networking Websites
4. Global News Media Search
5. OFAC – SDN List; Bank of England; Terrorist Exclusion List; EU Consolidated List
6. U.N. Security Council List of Terrorist Associated Entities
7. Independent Inquiry Committee Into the United Nations Oil-For-Food Program Report
8. "Golden Chain" List
9. Scandals Databases
10. U.S. Government Agency Most Wanted Lists
11. International Most Wanted Lists
12. U.S. Regulatory Databases
13. GSA Excluded Parties List
14. Terrorism Databases

The Contractor shall develop two different report forms. The first form will be an executive summary of each of the test cases' results. The second form will be a complete report of each of the test cases. In each form, the Contractor shall develop a method to remove all personal identifiable information.

After Government approval of the two report forms the Contractor shall uses these report forms to conduct their Open Source Research study on the 400 test cases.

The Contractor shall also provide an executive summary report and presentation to provide SPAWAR with the summary of the outcome of the results. This summary will include important findings discovered through out the study and any impacts the contractor believes to be important to this project.

The Contractor shall also host a two (2) day meeting with Government Personnel in Charleston, South Carolina.

6.2.1 Deliverable Products: The deliverable products for this task consist of the following:

a. A Draft and Final submission of the Complete report form. The Draft shall be submitted to the SPAWAR PE for review and comments. Following the incorporation of comments from the Draft submittal, the Contractor shall provide a Final submittal.
b. A Draft and Final submission of the Executive Summary report form. The Draft shall be submitted to the SPAWAR PE for review and comments. Following the incorporation of comments from the Draft submittal, the Contractor shall provide a Final submittal.
c. A Complete report and Executive Summary report on the 400 test cases. The reports shall be void of any personal identifiable information.
d. An Executive summary report in MS Word (latest version) format and an Executive Summary Presentation in MS Power Point (latest version) format. The Executive summary shall include the important finding, discoveries and implications through out the study as well as any impact the contractor believes to be important.
e. Host a two (2) day meeting with SPAWAR and other Government personnel in Charleston, SC.

6.2.2 Schedule: The schedule for this task shall be incorporated into the POA&M (Task A)

7. GOVERNMENT FURNISHED INFORMATION (GFI)

The following is a list of government furnished information:

a. Government approved biographical information on 400 test cases.

8. GOVERNMENT FURNISHED MATERIAL (GFM)

N/A.

9. GOVERNMENT FURNISHED EQUIPMENT (GFE)

N/A.

10. CONTRACTOR FURNISHED EQUIPMENT

N/A.

11. CONTRACTOR FURNISHED MATERIAL

N/A.

12. TRAVEL REQUIREMENTS

It is anticipated that travel to/from places of performance will be required.

13. TRANSPORTATION OF EQUIPMENT / MATERIAL

N/A.

14. DELIVERABLES

Deliverables provided electronically under this tasking shall be sent to the COR and the Project Engineer as identified in section 5 of this SOW.

Text Documents: Text document deliverables shall be submitted in black and white (color where appropriate) hard copy, bound, 8.5 by 11-inch standard size. Text Documents shall also be submitted in MS Word, MS Excel, MS PowerPoint and MS Project and/or Adobe Acrobat formats.

15. SUB-CONTRACTING REQUIREMENTS

Corporate Risk International (CRI) shall be subcontracted to perform investigative web scrubs detailed in section 6.2. CRI has existing subject matter experts and system tools/resources required to complete this tasking in the time required.

16. ACCEPTANCE PLAN

Work performed, materials and task data to be submitted under this delivery order will be made available to be inspected for compliance with this D.O. and accepted by the COR or authorized representative as specified herein.

17. OTHER CONDITIONS / REQUIREMENTS

Contractors will be required to sign a Non-Disclosure Agreement for the products produced and methods used during this project. All products and information gathered during the course of this project will be turned over to SPAWAR.

18. LIST OF ATTACHMENTS

Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

The contractor, ____, and its employee, ____________________________________, recognize that in the performance of Contract Number______________________________, Delivery Order__________, the contractor and its employee will become knowledgeable of government information. In consideration of being given access to information required to perform the contract, it is specifically agreed that neither the contractor nor its employee, will use, release, or disclose in whole or in part outside the government, information made known to it by the performance of this contract without the express, written authorization of the Contracting Officer.

It is agreed that the employee's obligations contained in this agreement apply to the unauthorized use/disclosure of information to his employer (the contractor) or a competing contractor and may not be used by the employee for competitive, commercial, employment-related or personal advantage.

FOR THE CONTRACTOR:

____ ________________
(Signature) (Date)

EMPLOYEE:

____ ________________
(Signature) (Date)

(U//~~FOUO~~) Office of the Director of National Intelligence
Special Security Center

(U//~~FOUO~~) Open Source Research Project Privacy Response

Submitted: April 01, 2008

Version: 1.0

Prepared By:

Corporate Risk International (CRI)®

(U) This document contains information exempt from mandatory disclosure under the FOIA, and withheld from public release until approved for release by the originator.

TABLE OF CONTENTS

SECTION I: PREDICATION/REQUEST FOR INFORMATION

Corporate Risk International (CRI) understands that SPAWAR requires follow up information related to CRI's July 27, 2007 proposal to provide Open Source Research as part of a background screening test program. CRI has been requested to provide a privacy disclaimer statement, research methodology summary and general information regarding the social networking sites that will be researched. CRI further understands that this test program will be strictly limited to open source and Internet-based research only. Additionally, CRI understands that third party privacy must be maintained during all aspects of this research project.

SECTION II: CRI PRIVACY DISCLAIMER

To prevent unauthorized access, maintain data integrity, and ensure the proper legal use of information, Corporate Risk International (CRI) has instituted appropriate physical, electronic, and managerial procedures to safeguard and secure the information with which CRI is entrusted.

With regard to the Open Source Research project, CRI will gather and maintain information for the sole use and benefit of our client, the Department of the Navy. Data collected by CRI will be via open source, publicly available means, and only regarding individuals who have provided written consent to participate in this research.

Information that is collected regarding the subject that also contains mention of a third party individual will be reviewed by CRI only for pertinent information regarding the subject. Only relevant information regarding the subject will be maintained by CRI. Every effort will be made to minimize review of portions of records that pertain to third party individuals. This type of review will occur only when it is necessary to understand the context in which information related to the subject appears.

SECTION III: CRI RESEARCH METHODOLOGY

Step-By-Step Guideline for Open Source Screening Matters

1) The request is received from the client. The matter is then assigned to a case manager and a case is opened.

2) A review of appropriate local and national media will be conducted to identify if the participant has been the subject of noteworthy / adverse media coverage.
    a. A keyword search will be utilized to narrow down the results to adverse or noteworthy information.

3) Checks will be conducted of the Internet (via Google-type search engines) to determine whether the subject has a publicly-accessible online profile.

4) There are a number of social, professional and special interest networking sites that allow users to create and post publicly-available profiles, photos and blogs. While many of these websites provide options for users to set privacy settings to block public access, many users intentionally make their profiles available for public viewing.

    For this research project, searches will be conducted to identify publicly-available profiles or blogs posted by participants providing written consent. Searches will be conducted using the proper name of the individual, variations of the proper name ("Thomas Doe" will be searched "Tom Doe" and "Tommy Doe"), known email addresses (TomDoe22181@yahoo.com), and variations of the known email addresses (TomDoe22181). Searches will be strictly limited to publicly-accessible sites and or social networking sites where there is no expectation of privacy.

    CRI regularly uses their own preexisting site accounts to provide access to social networking site search engines and/or the ability to view other user profiles. Profiles of these CRI accounts provide truthful representations of CRI researchers. No attempts will be made to obtain information that is not publicly-accessible, to solicit invitations to become part of a subject's network, or to make any attempt to view password-protected information. Furthermore, no third party links will be followed as part of this research project (see third paragraph in Section II).

    Popular social networking websites to be utilized in this research include, but are not limited too: Doostang.com, Facebook.com, Friendster.com, KickStart.com, Linkedln.com, or MySpace.com. Listed below are site accessibility descriptions.

    a. **Doostang (www.doostang.com).** Doostang describes itself as an "online career community that connects people (anyone age 18 or older) through personal relationships and affiliations." Users not only use Doostang to interact with one another, but also as a forum to post jobs and recruit potential employees. User profiles are publicly-available to all other Doostang users and often list educational and professional credentials, resumes and endorsements. No attempts will be made to misrepresent CRI researchers or to search in any area other than those allowable. (Full terms of the Doostang.com user agreement can be found at: http://www.doostang.com/privacypolicy.asp)

b. **Facebook (www.facebook.com).** Facebook is a popular social networking site for use by individuals age 13 and older. Regardless of privacy settings, Google-type searches generally yield limited information of a Facebook user profiles. Furthermore, common privacy settings limit other Facebook users from being able to view profiles. Only a limited amount of information contained in Facebook profiles is available to users. For the purposes of this research project, CRI will not attempt to search in any area other than those allowable by a user's security settings. "Public profiles" open to non-Facebook users, however, will be reviewed. (For terms of use see (http://www.facebook.com/terms.php)

c. **Friendster (www.friendster.com).** Friendster.com is a social networking site very similar to Myspace. Friendster.com is geared to an international audience for individuals of any age. Profiles of Friendster users are searchable via Google-type search engines or directly from the Friendster website. Like MySpace, individuals can limit their profile's access by applying security settings. For the purposes of this research project, CRI will not attempt to search in any area other than those allowable by a user's security settings. (Full terms of the MySpace.com user agreement can be found at: http://www.friendster.com/info/tos.php.)

d. **KickStart (http://kickstart.yahoo.com).** Kickstart is a Yahoo!-based professional networking site designed for college students, alumni, and professionals. KickStart profiles are publicly-available and searchable via Google-type search engines by users and non-users. Profiles often contain educational and professional credentials. For the purposes of this research project, CRI will not attempt to search in any area other than those allowable. (For terms of use and privacy policy see http://info.yahoo.com/privacy/us/yahoo/kickstart/)

e. **LinkedIn (www.linkedin.com).** LinkedIn is a professional networking site used by individuals (anyone age 18 or older), to strengthen professional networks. Users often list educational and professional credentials in publicly-available basic profiles which are searchable via Google-type search engines. More comprehensive publicly-available profiles are viewable by other users of the site. For the purposes of this research project, CRI will conduct searches using pre-existing CRI LinkedIn accounts. No attempts will be made to misrepresent CRI researchers or to search in any area other than those allowable. (Full terms of the LinkedIn.com user agreement can be found at: http://www.linkedin.com/static?key=user_agreement)

f. **MySpace (www.myspace.com).** MySpace is a social networking site that is geared to an international audience of individuals 14 years and older. Profile pages may consist of various types of information including name, date of birth, address, hobbies, interests, education, and profession. Profile pages may also include photos and publicly-viewable written exchanges. It is important to note that MySpace users can set security settings that prohibit their profile form being viewed by those other than pre-designated "Friends.' For the purposes of this research project, CRI will not attempt to search in any area other than those allowable by a user's security settings. (Full terms of the MySpace.com user agreement can be found at: http://www.myspace.com/index.cfm?fuseaction=misc.terms).

5) Results of steps 2-5 will be reported to client per July 2007. All personally identifying information will be retracted from such reports so as to maintain anonymity of the subject. Data will be destroyed by CRI per the client's wishes.

CRI Compliance Training

All CRI employees receive bi-annual compliance training and must sign and adhere to the following guidelines when conducting research:

As an employee with CRI, you must comply with all applicable laws and regulations, and you are prohibited from engaging in any actions that would reflect negatively on CRI and/or its clientele, including without limitation the following:

a) Violation of privacy and credit laws and other laws protecting the confidentiality of financial or other personal information;
b) Misappropriation of trade secrets or proprietary information;
c) Misrepresenting oneself as an agent of a governmental authority;
d) Interfering with a government investigation;
e) Bribery or making other illegal payments;
f) Defamation;
g) Physical and electronic surveillance or taping of conversations;
h) Trespassing;
i) Gaining unauthorized access to physical or electronic records;
j) Accessing discarded personal or commercial records and other acts considered to be an invasion of privacy; and
k) Direct contact (verbal or otherwise) with subject companies or individuals under review.

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 13

1. CONTRACT/PURCH. ORDER/ AGREEMENT NO.
N65236-05-D-7148

2. DELIVERY ORDER/ CALL NO.
0194

3. DATE OF ORDER/CALL (YYYYMMMDD)
2008 Jun 30

4. REQ./ PURCH. REQUEST NO.
N652368176C015

5. PRIORITY

6. ISSUED BY CODE N65236

SPAWAR SYSTEMS CENTER CHARLESTON
PO BOX 190022 TEAM 7
843-218-5860
JENNIFER.KELLEY@NAVY.MIL
NORTH CHARLESTON SC 29419-9022

7. ADMINISTERED BY *(if other than 6)* CODE S2404A

DCMA VIRGINIA
10500 BATTLEVIEW PARKWAY
SUITE 200
MANASSAS VA 20109-2342

8. DELIVERY FOB
☒ DESTINATION
☐ OTHER
(See Schedule if other)

9. CONTRACTOR CODE 3K773 FACILITY

NAME AND ADDRESS
M.C. DEAN, INC.
GOVERNMENT REPRESENTATIVE
DBA: MCDEAN
22461 SHAW ROAD
DULLES VA 20166-2461

10. DELIVER TO FOB POINT BY (Date) (YYYYMMMDD)
SEE SCHEDULE

11. MARK IF BUSINESS IS
☐ SMALL
☐ SMALL DISADVANTAGED
☐ WOMEN-OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Schedule

14. SHIP TO CODE

SEE SCHEDULE

15. PAYMENT WILL BE MADE BY CODE HQ0338

DFAS-COLUMBUS CENTER
DFAS-COLUMBUS CTR; SOUTH ENTITLEMENT DIVI
P. O. BOX 182264 EFT:T
COLUMBUS OH 43218-2264

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER	DELIVERY/ CALL	X	This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
	PURCHASE		Reference your quote dated Furnish the following on terms specified herein. REF:

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR　SIGNATURE　TYPED NAME AND TITLE　DATE SIGNED (YYYYMMMDD)

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/ LOCAL USE

See Schedule

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/ SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

** If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.*

24. UNITED STATES OF AMERICA
TEL: 843-218-5944
EMAIL: sharon.marince@navy.mil
BY: SHERRY MARINCE

Sharon A. Marince
CONTRACTING / ORDERING OFFICER

25. TOTAL $234,822.00

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

c. DATE (YYYYMMMDD)

d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

28. SHIP NO.

29. DO VOUCHER NO.

30. INITIALS

☐ PARTIAL
☐ FINAL

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

f. TELEPHONE NUMBER

g. E-MAIL ADDRESS

36. I certify this account is correct and proper for payment.

a. DATE (YYYYMMMDD)

b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

31. PAYMENT
☐ COMPLETE
☐ PARTIAL
☐ FINAL

34. CHECK NUMBER

35. BILL OF LADING NO.

37. RECEIVED AT

38. RECEIVED BY

39. DATE RECEIVED (YYYYMMMDD)

40. TOTAL CONTAINERS

41. S/R ACCOUNT NO.

42. S/R VOUCHER NO.

Section B - Supplies or Services and Prices

ITEM NO	SUPPLIES/SERVICES	EST QUANTITY	UNIT	UNIT PRICE	TOTAL AMOUNT
0011		31,479		$1.00	$31,479.00
	LABOR CATEGORIES - SECOND OPTION YEAR				
EXERCI SED OPTION					
	ACRN AA CIN: N652368176C0150011 PURCHASE REQUEST NUMBER: N652368176C015				

ITEM NO	SUPPLIES/SERVICES	EST QUANTITY	UNIT	UNIT PRICE	TOTAL AMOUNT
0012		1,635		$1.00	$1,635.00
	MATERIALS/ELECTRONIC EQUIPMENT				
EXERCI SED OPTION					
	PURCHASE REQUEST NUMBER: N652368176C015				

ITEM NO	SUPPLIES/SERVICES	EST QUANTITY	UNIT	UNIT PRICE	TOTAL AMOUNT
0014		201,708		$1.00	$201,708.00
	OTHER ODCS				
EXERCI SED OPTION					
	PURCHASE REQUEST NUMBER: N652368176C015				

ITEM NO	SUPPLIES/SERVICES	EST QUANTITY	UNIT	UNIT PRICE	TOTAL AMOUNT
0015					NSP
	DD1423 CONTRACT DATA REQUIREMENTS LIST				

Section C - Descriptions and Specifications

SOW
SHORT TITLE: ODNI Open Source Research Project

1. PLACE(S) OF PERFORMANCE

a. SPAWAR Designated Facilities
b. Corporate Risk International, CRI
c. MC Dean, Chantilly, VA
d. ODNI Special Security Center (SSC)

2. REFERENCES

The latest revision of the following guidance documents forms a part of this SOW. In cases where documentation conflicts, for clarification, the SPAWAR Project Manager shall be notified, in writing, and shall make the final determination.

a. Standard Form 86 – Questionnaire for National Security Positions
b. Privacy Act – 5 USC 552a(b)
c. Latest ODNI Open Source Project Privacy Response

3. SPECIFICATIONS

NONE

4. SECURITY REQUIREMENTS

a. Maximum required clearance is SECRET.
b. All visit requests shall be forwarded to the place of performance via the SPAWAR Systems Center Charleston Technical Point of Contact for certification of the "Need-To-Know". All requests shall contain the information required by the NISPOM and shall not exceed the completion date of this order. The DD-254 of the basic contract applies.
c. Government issued personal information shall be protected as required by privacy act and destroyed at the completion of this task. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction. Inappropriate disclosure, lost, stole, or compromised Privacy Act data shall be reported to the SPAWAR PE immediately. Deliverables that include Privacy Act data shall be marked as "For Official Use Only - Privacy Act Data" at the top and bottom of each page.

5. COR DESIGNATION

The COR for this delivery order is b(6), who can be reached at (843) 218-4439 or e-mail: b(6). The SPAWAR project engineer that has a specific interest in this work is b(6), who can be reached at (843) 218-4080.

6. DESCRIPTION OF WORK

Project Background: The Office of the Director of National Intelligence (ODNI) Special Security Center (SSC) Research program coordinates, conducts and oversees research in the area of personnel security to include issues relating to investigations, adjudications and polygraph. Research is conducted at high level and depending on the area of research with participation with Government and non-Government research organizations.

The Intelligence Reform and Terrorism Prevention Act of 2005 mandates the "use of available technology in clearance investigations and adjudications". In support of the Intelligence Reform and Terrorism Prevention Act of 2005, the Director of National Intelligence considers personnel security a high priority and it is a major objective of his "100 Day Plan for Integration and Collaboration" to Modernize Business Practices and apply best practices to the personnel security arena. In recent years, the expanded use of the internet and the upsurge in social networking websites have added new concerns to the personnel security process and a new dimension to investigating a person's background and behavior.

Project Overview: The scope and nature of this study is "fact finding" to determine if meaningful personal information may be obtained from open source websites to determine if social behavior, often referred to as social networking in the cyber world, may reflect personal information that may be deemed as unprofessional, unethical or unacceptable to an employer (government agency). The study will also focus on the content of information that may be posted on open websites or "chat rooms" to determine if sensitive or classified information has been posted or transmitted via an unauthorized communication source.

This SOW covers the effort involved to perform such a study as described above and provide a report based on the findings. Tasks include the following:

a. Project Management

b. Statistical Study

6.1 Task A – Project Management

Task Description: The Contractor shall develop documentation outlining the baseline project approach to the ODNI SSC Program Manager within ten working days after funds are received. Within the baseline project approach, the contractor shall articulate the data/information required from the sponsor in order to complete the project. The POA&M shall include deliverables to be provided as specified in this SOW and must show completion of the tasking contained, to include all review periods for the documents produced. The Contractor shall update this schedule monthly using an Actual versus Baseline tracking method.

6.1.1 Deliverable Product: The deliverable products for this task shall consist of the following:

a. Plan of Action and Milestones (Microsoft Project) – Baseline Submission
b. Plan of Action and Milestones (Microsoft Project) – Monthly Submissions

6.1.2 Task Schedule: The Contractor shall receive approval of the POA&M from the Government prior to beginning work on the other tasks in this SOW. The Government will notify the Contractor within three (3) working days with approval or changes to the POA&M. An updated version of the POA&M shall be delivered with each monthly status report submission using an Actual versus Baseline tracking basis and provide the SPAWAR Project Manager (PM) with an electronic copy of the updated POA&M. The updated POA&M shall identify tasks, dependencies, actual start dates, durations, actual finish date, slippage, percent complete, and resources.

6.2 Task B – Statistical Study

Task Description: The primary goal of the "study" is to determine if social networking websites provide relevant information regarding the personal conduct of an individual that could reflect lack of professional or unethical behavior, potential criminal or statutory misbehavior, or the unauthorized publication of sensitive or even classified U.S. Government information. Based on the study a statistical analysis will be conducted to determine if the information collected may offer new methodologies for collecting and monitoring the behavior of employees that goes beyond the traditional inquiries conducted during the background and re-investigative process. The final report will provide conclusions and a next step as appropriate.

SPAWAR will provide the contractor with biographical information on 400 individuals limited to name, SSN, Place of Birth, Date of Birth for the test cases included in this study. Test cases will be selected pseudo-randomly from the Intelligence Community. Some specific common name test cases (i.e. Joseph Smith) may be selected to evaluate. All Government issued test cases issued for conducting due diligence inquiries via social networking websites will have completed and signed a Standard Form 86 (Questionnaire for National Security Positions), and have a completed Single Scope Background Investigation. The investigation will cover, at a minimum, Facebook, MySpace, and U-Tube web logs or "blogs" that may be appropriate to referenced test cases. 400 test cases will be provided to the contractor to perform the above investigations on. A list of the databases that must be searched include the following:

1. Global Internet Search
2. Internet "Blog" Websites
3. Internet Social Networking Websites
4. Global News Media Search
5. OFAC – SDN List; Bank of England; Terrorist Exclusion List; EU Consolidated List
6. U.N. Security Council List of Terrorist Associated Entities
7. Independent Inquiry Committee Into the United Nations Oil-For-Food Program Report
8. "Golden Chain" List
9. Scandals Databases
10. U.S. Government Agency Most Wanted Lists
11. International Most Wanted Lists
12. U.S. Regulatory Databases
13. GSA Excluded Parties List
14. Terrorism Databases

The Contractor shall develop two different report forms. The first form will be an executive summary of each of the test cases' results. The second form will be a complete report of each of the test cases. In each form, the Contractor shall develop a method to remove all personal identifiable information.

After Government approval of the two report forms the Contractor shall uses these report forms to conduct their Open Source Research study on the 400 test cases.

The Contractor shall also provide an executive summary report and presentation to provide SPAWAR with the summary of the outcome of the results. This summary will include important findings discovered through out the study and any impacts the contractor believes to be important to this project.

The Contractor shall also host a two (2) day meeting with Government Personnel in Charleston, South Carolina.

6.2.1 <u>Deliverable Products:</u> The deliverable products for this task consist of the following:

a. A Draft and Final submission of the Complete report form. The Draft shall be submitted to the SPAWAR PE for review and comments. Following the incorporation of comments from the Draft submittal, the Contractor shall provide a Final submittal.
b. A Draft and Final submission of the Executive Summary report form. The Draft shall be submitted to the SPAWAR PE for review and comments. Following the incorporation of comments from the Draft submittal, the Contractor shall provide a Final submittal.
c. A Complete report and Executive Summary report on the 400 test cases. The reports shall be void of any personal identifiable information.

d. An Executive summary report in MS Word (latest version) format and an Executive Summary Presentation in MS Power Point (latest version) format. The Executive summary shall include the important finding, discoveries and implications through out the study as well as any impact the contractor believes to be important.

e. Host a two (2) day meeting with SPAWAR and other Government personnel in Charleston, SC.

6.2.2 Schedule: The schedule for this task shall be incorporated into the POA&M (Task A)

7. GOVERNMENT FURNISHED INFORMATION (GFI)

The following is a list of government furnished information:

a. Government approved biographical information on 400 test cases.

8. GOVERNMENT FURNISHED MATERIAL (GFM)

N/A.

9. GOVERNMENT FURNISHED EQUIPMENT (GFE)

N/A.

10. CONTRACTOR FURNISHED EQUIPMENT

N/A.

11. CONTRACTOR FURNISHED MATERIAL

N/A.

12. TRAVEL REQUIREMENTS

It is anticipated that travel to/from places of performance will be required.

13. TRANSPORTATION OF EQUIPMENT / MATERIAL

N/A.

14. DELIVERABLES

Deliverables provided electronically under this tasking shall be sent to the COR and the Project Engineer as identified in section 5 of this SOW.

Text Documents: Text document deliverables shall be submitted in black and white (color where appropriate) hard copy, bound, 8.5 by 11-inch standard size. Text Documents shall also be submitted in MS Word, MS Excel, MS PowerPoint and MS Project and/or Adobe Acrobat formats.

15. SUB-CONTRACTING REQUIREMENTS

Corporate Risk International (CRI) shall be subcontracted to perform investigative web scrubs detailed in section 6.2. CRI has existing subject matter experts and system tools/resources required to complete this tasking in the time required.

16. ACCEPTANCE PLAN

Work performed, materials and task data to be submitted under this delivery order will be made available to be inspected for compliance with this D.O. and accepted by the COR or authorized representative as specified herein.

17. OTHER CONDITIONS / REQUIREMENTS

Contractors will be required to sign a Non-Disclosure Agreement for the products produced and methods used during this project. All products and information gathered during the course of this project will be turned over to SPAWAR.

18. LIST OF ATTACHMENTS

Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

The contractor, ____, and its employee, ____, recognize that in the performance of Contract Number_______________________________, Delivery Order__________, the contractor and its employee will become knowledgeable of government information. In consideration of being given access to information required to perform the contract, it is specifically agreed that neither the contractor nor its employee, will use, release, or disclose in whole or in part outside the government, information made known to it by the performance of this contract without the express, written authorization of the Contracting Officer.

It is agreed that the employee's obligations contained in this agreement apply to the unauthorized use/disclosure of information to his employer (the contractor) or a competing contractor and may not be used by the employee for competitive, commercial, employment-related or personal advantage.

FOR THE CONTRACTOR:

______________________________________ ______________
(Signature) (Date)

EMPLOYEE:

______________________________________ ______________
(Signature) (Date)

Section E - Inspection and Acceptance

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
All	Government	Destination	Government	Government

Section F - Deliveries or Performance

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS
All	POP 30-JUN-2008 TO 30-SEP-2008		FOB: Destination

Milestone Payment Schedule

Payment requisitions will be made in accordance with the following milestone schedule:

MS	Description	CLIN 0011 Labor	CLIN 0012 ODCs-Material / Equipment	CLIN 0014AA ODCs Misc. Subcontractor	CLIN 0014AB ODCs Not Stipulated	Total
1	POA&M, Planning, and Start-Up	$ 6,365.00	$ 1,635.00	$ 27,000.00		$ 35,000.00
2	Month 1 Research Complete	$ 7,000.00		$ 53,000.00		$ 60,000.00
3	Month 2 Research Complete	$ 7,000.00		$ 53,000.00		$ 60,000.00
4	Month 3 Research Complete	$ 7,000.00		$ 53,000.00		$ 60,000.00
5	Final Documentation & Government Acceptance	$ 4,114.00		$ 15,600.00	$ 108.00	$ 19,822.00
	Total	**$31,479.00**	**$ 1,635.00**	**$ 201,600.00**	**$ 108.00**	**$ 234,822.00**

Section G - Contract Administration Data

ACCOUNTING AND APPROPRIATION DATA

AA: 1781319 F999 00E 41756 0 068941 000000
COST CODE: 520010970000
AMOUNT: $234,822.00
CIN N652368176C0150011: $234,822.00

CLIN	JOB ORDER	FUNDS EXP. DATE	DOC:	REQ:
ALL	ADHYEX8A02	30-SEP-2008	N4175608WX50306/AA	N65236-8176-C015

Section H - Special Contract Requirements

DIST

The contractor shall follow the invoicing instructions included in Clause G-317 WAWF of the basic contract.

M. C. Dean 3725 Concorde Pkwy, Suite 100 Chantilly, VA 20151 Nancy.Gordon-Brooks@mcdean.com	DCAA Fairfax Branch Office Building 2, Suite 315 171 Elden Street Herndon, VA 20170-4810
DCMA Virginia 10500 Battleview Parkway, Suite 200 Manassas, VA 20109 COR: b(6), Code 743WH b(6)	DFAS COLUMBUS CENTER DFAS-CO/South Entitlement Division P O BOX 182264 EFT:T COLUMBUS OH 43218-2264 SPAWAR Codes: 0123 Finance Originator: b(6) Code 56430EA

UNCLASSIFIED

Considering Web Presence in Determining Eligibility to Access Classified Information: A Pilot Study

[redacted] Ph.D. & [redacted] Psy.D. b6

Office of the Director of National Intelligence, Special Security Center

INTRODUCTION

Personnel within the Intelligence Community (IC) are required to handle information that has the potential to harm national security. Eligibility to access classified information is provided after a determination that personnel are an acceptable security risk, which is established through a voluntary and thorough evaluative process.[1]

The ubiquity of information technologies has posed new challenges to security screening IC personnel. While screening applicants' web presence has shown to be a growing practice in industry[2] there appear to be no studies have examined the utility of evaluating applicants for purposes of personnel security evaluations.

OBJECTIVE

This pilot study is an exploratory and consensual effort to examine information associated with applicants' web presence and its relevance to personnel security.

METHOD

Participants were 349 (Mean age = 40.5, SD =13.1, 68% male) government and contractor applicants from two US IC agencies. All participants initiated personnel security processing at the time of recruitment and were subject to thorough informed consent procedures prior to participation.

Industry partner analysts (Corporate Risk International©) searched publicly-available internet information including blogs, social networking sites (SNSs), bulletin boards and media sites using variations of applicants' names and email addresses. No attempts were made to access password protected information. Once collected, data was anonymized.

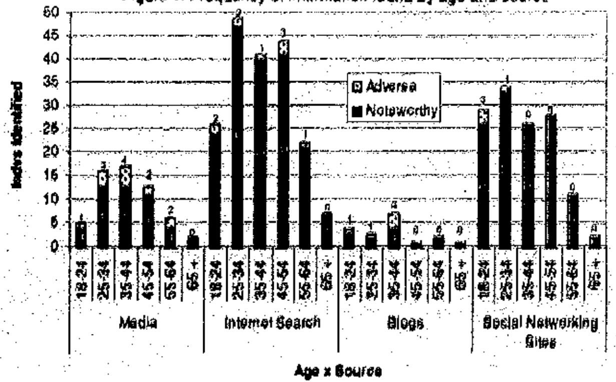
Two raters judged the significance of information (none/general, noteworthy, adverse) based on descriptions or depictions of illegal activity, disclosure of sensitive information or postings indicative of questionable judgment.

Raters also judged the degree to which found information was likely related to the participant based on known demographic information (credible, possible, unlikely). Instances of disagreement were resolved by an expert analyst. Only information deemed credible was subject to subsequent analysis.

RESULTS

Credible security-relevant information was found in 67% (n=235) of searches. Of that, information judged to be adverse was found in only 12% (n=30) of cases.

Figure 1. Frequency of information found by age and source



Significantly more noteworthy info was uncovered with SNSs (n=111) and Internet searches (n=53; *Cochran's Q* (3) = 251, *p* <.001). The amount of adverse info uncovered, however, did not differ across sources (*Cochran's Q* (3) = 6, *p* =.112).

While trends suggest that greater amounts of noteworthy information are uncovered across middle age groups, small cell sizes prohibited inferential analysis of these findings.

DISCUSSION

Results suggest that while applicants' web presence provides a significant amount of noteworthy information- especially via internet searches and SNSs- it provides only a small amount of credible adverse information. The nature of this information, however, may be of potential value, either as a tool to confirm information obtained using other strategies or to provide investigative leads.

Follow-up studies should utilize larger samples, qualitatively explore the types and severity of adverse information gathered, use objective criteria to ensure fidelity of information, and ensure reliability of rater judgments where necessary.

LIMITATIONS

- The qualitative nature of adverse and noteworthy info is limited.
- Limitations in interpretability due to small sample size.
- Sample bias was introduced by extensive informed consent procedures and applicant self-selection. Validity of data may be in question due to participants' ability to alter web presence prior to data collection.
- Validity of information was not corroborated and inter-rater reliability of ratings is not known.

SELECTED REFERENCES

1. Office of the Director of National Intelligence (October, 2008). Intelligence Community Directive 704, *Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Programs*. Washington, DC.

2. CareerBuilder.com (2008, September 10). 'One-in-Five Employers Use Social Networking Sites to Research Job Candidates. Retrieved June 16, 2009, from http://www.msca.edu/careercentral/pdfs/One-in-Five_Employers_Use_Social_Networking_Sites_to_Research_Job_Candidates.pdf

For more information contact [redacted] PhD: [redacted]

UNCLASSIFIED

DNI Special Security Center Research Program

b6 [redacted] Psy.D.
Research Program Manager
DNI Special Security Center

Predication & Project Description

Description & Predication

- Study to determine if meaningful personal information may be obtained from open source websites to determine if social behavior, often referred to as social networking, may reflect personal information that may be deemed as unprofessional, unethical or unacceptable to an employer (government agency).
- Research conducted on 349 “Test Cases” or “Subjects” who currently hold clearances.
- Deliverables – Executive Summaries & Report Forms for Test Cases 001 – 349 & Summary Report of Findings and Analysis.

Methodology

Open Source Research

- Media Research
- Internet Research
- Blog Research
- Social Networking

  MySpace
  Friendster
  LinkedIn
  Doostang
  Kickstart
  YouTube
  Facebook
- Global Compliance

Methodology

Name Match Issue

- Additional research conducted to reduce name matches (due to limited profiles - names, dates of birth, social security numbers, and addresses).
- Research conducted to obtain past addresses.
- For extremely common names - searches and reporting of results were limited to the geographic areas that CRI was able to confirm to be associated with the subject.
- However, address history obtainable by CRI is generally limited to a seven to ten year period.

Methodology

Characterization of Results

Prior to initiation of research, parameters for each characterization of results were established.

- **Description of No Information Found** – No public reference to subject.
- **Description of General Information Found** – Subject's name appears in public information, including media references and biographical information on corporate websites not posted by the subject. Information includes biographical information as posted on professional networking sites, such as LinkedIn.
- **Description of Noteworthy** – Inadvertent or deliberate posting of personal information and/or inclusion of "questionable" material – i.e. possible underage drinking, profanity, extreme religious and/or political views on public forums. Also includes personal blog websites or photo websites that could be easily attributable to the subject. For example, the personal blog/website also includes information about the subject's professional career/employer or includes contact information or home address that would allow the subject to be easily contacted.
- **Description of Adverse** – Deliberate and overly descriptive posting of personal and/or work related information on public forums. This includes information about the subject's specific work assignment, including listing descriptive information about colleagues and/or work site. Adverse classifications were also applied when references were found indicating illegal drug use or pictures appearing to show the subject engaging in illegal drug use.

Methodology

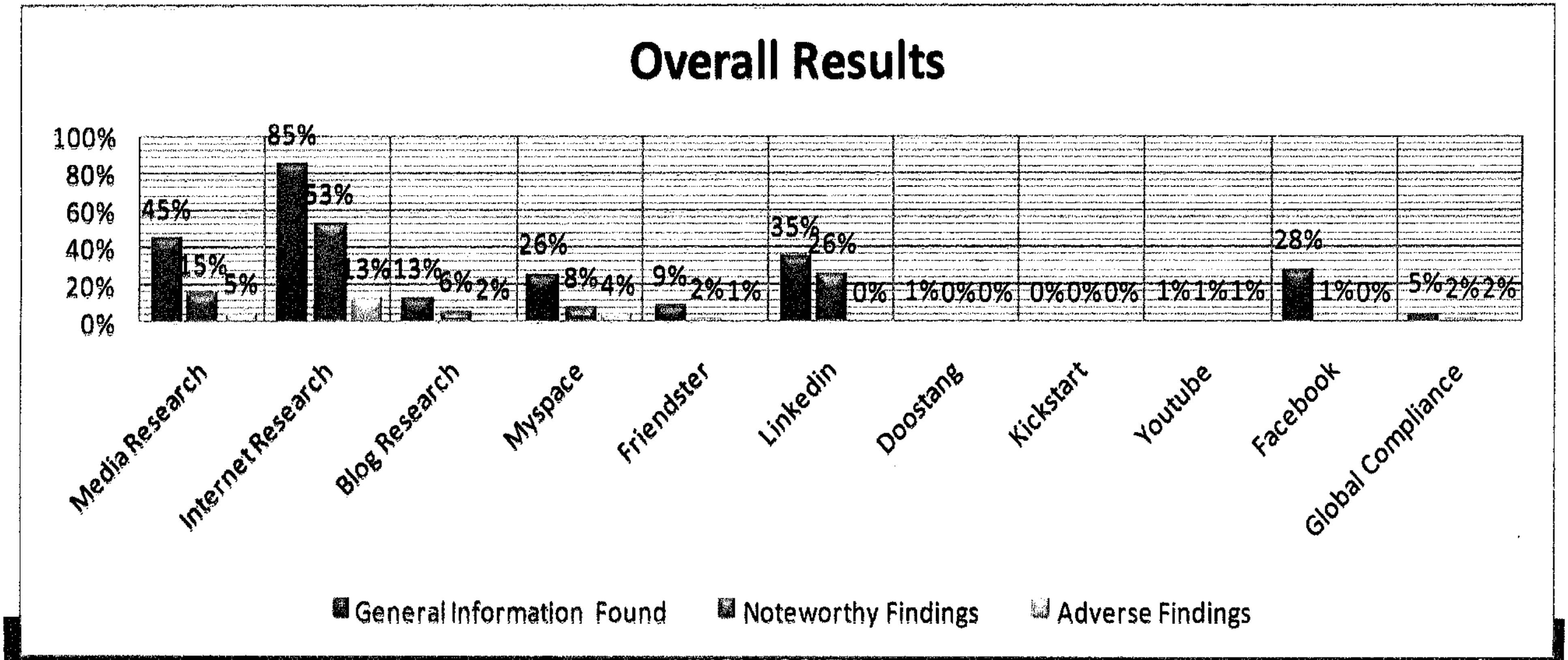
Key Limitations

- Limited information provided – did not allow for identification of e-mail addresses/screen names.
- Several name matches due to commonality of subject names/lack of application detail.
- Advance warning of research/signed consent form/may have allowed applicants to remove questionable materials.
- Lack of profile information provided did not allow for research to identify discrepancies and/or omissions from subjects' applications.

Analysis

Top Producing Categories

General :	Internet, Media, LinkedIn
Noteworthy:	Internet , LinkedIn, Media
Adverse:	Internet, Media, MySpace



Analysis

Search String Analysis

Most Productive:

- Internet
- Media Research
- LinkedIn
- MySpace/Facebook
- Blog Research

Limited Findings/Omit:

(produced results for less than 5-10% of subjects)

- Doostang
- KickStart (inactive)
- YouTube
- Global Compliance
- Friendster

Analysis

Analysis of Findings by Age Range

- Reviewed to determine if Open Source research produced more noteworthy or adverse results among certain age groups. Also focused on whether certain strings produced more pertinent results within age groups.

Age Range	Category	Number of Subjects
- age 18-24	A	58 subjects assigned
- age 25-34	B	77 subjects assigned
- age 35-44	C	77 subjects assigned
- age 45-54	D	85 subjects assigned
- age 55-64	E	39 subjects assigned
- age 65 +	F	10 subjects assigned
- n/a		3 unable to qualify

Analysis

Age Range Findings – General Results

- Limited differences across age ranges for Internet Research. General results were found during Internet Research for 80% or more of the subjects.

- Media Research produced General Results for 38 – 62% of the subjects across all age ranges.

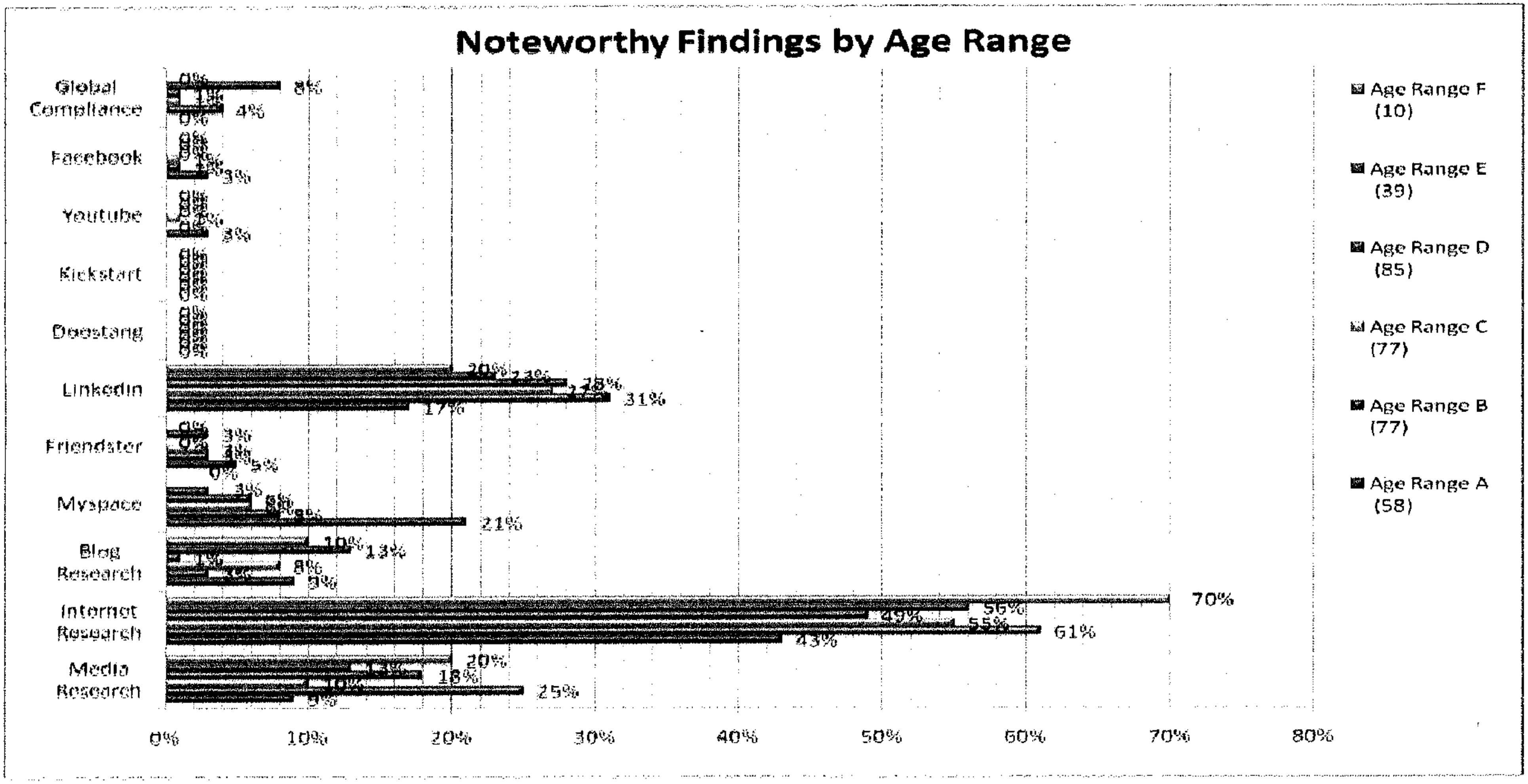
- Blog Research was also fairly consistent across age ranges, with General Results being found for between 7-20% of subjects.

- Social Networking sites (MySpace, Friendster, and Facebook) found that the percentages of General Results generally decrease as a subject's age increases.

- General Results were fairly consistent for professional networking site LinkedIn, with the lowest amount of findings in the youngest age category at 26% to the highest percent of findings, 42%, for subjects in the 25-34 age categories.

Analysis

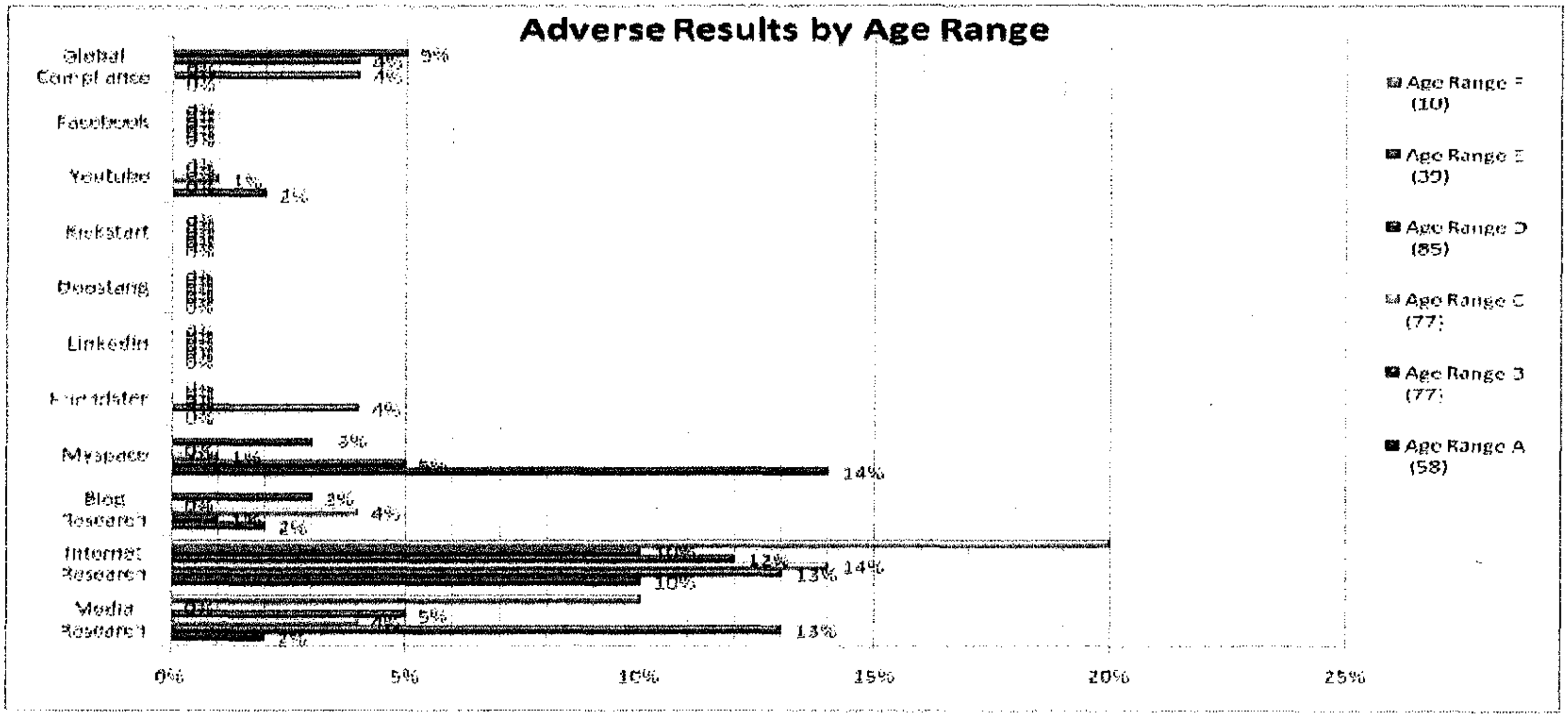
Age Range Findings – Noteworthy



Analysis

Age Range Findings – Adverse

- Consistent across age ranges for Media, Blog and Internet research.
- Highest percentage of Adverse Findings for research of Social Networking sites was in age group A (18 -24).
- In age range E (55-64) adverse findings were found for 3% of the 39 subjects Social Networking /MySpace.



Analysis

- **Adverse Analysis**
  - Review of all Adverse (across age range/research category) – 13% of Adverse considered 'possible illegal activity'.
  - Approximately 48% of subjects with Adverse findings could be classified as having 2 or more pieces of Adverse or Noteworthy References.
  - However, due to prevalence of name matches, it is difficult to determine if the multiple pieces of adverse or noteworthy information can be attributable to the same subject.

Findings & Recommendations

Key Findings

- Review of subjects' public profile may allow for a more complete overview of subjects' background, activity, etc. to assist the adjudicator conducting the background screening.
- Useful for re-investigations and for periodic investigations on active clearance holders to determine if any key changes have occurred in subjects' lifestyle and/or activities.
- Allow adjudicators to alert active clearance of holders of possible sensitive information online.
- Allow adjudicators to identify 'friends' through networking sites for field interview.
- Identify issues or concerns not developed during the standard clearance process.

Findings & Recommendations

Recommendations

- Identify sites most useful for conducting open source research.

  Media Research

  Internet Research

  Blog Research

  Social Networking – MySpace, Facebook

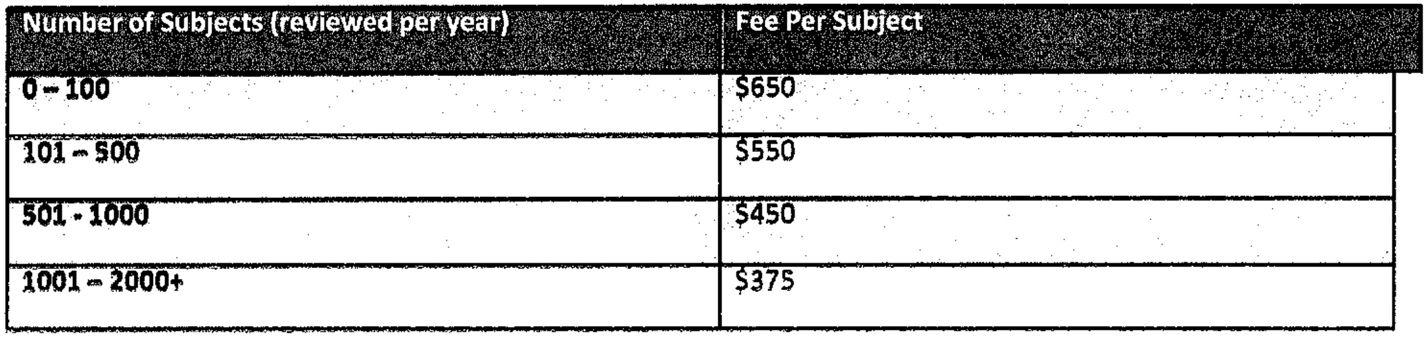
  Professional Networking – LinkedIn

  Explore Twitter – Fastest Growing Social Networking Site

- Supply profiles/applications to Open Source vendors to rule out name matches and identify omissions.
- Make a first step in the clearance process to allow inquiry to be tailored.
- Consider using as a means to validate/cross-check accuracy of standard clearance (note recent article regarding falsification of clearance information).
- Incorporation due to affordability/quick turnaround (identify key issues prior to lengthy/costly clearance process).
- Incorporation due to industry standard.

Requirements & Fees

- **Fee Structure/Researcher Requirements**
  - Experienced researchers require 2-4 weeks formal training followed by 6 months on the job training.
  - Research Team for developing new open source resources, always evolving, utilizing proprietary techniques.
  - Best researchers are highly Internet savvy.
  - Sample fee structure:



Number of Subjects (reviewed per year)	Fee Per Subject
0 – 100	$650
101 – 500	$550
501 - 1000	$450
1001 – 2000+	$375

- **Questions & Answers**

Corporate Risk International

Final Report & Analysis

[Open Source Research Project]

Prepared for [redacted]
SPAWAR Atlantic
June 10, 2009

Prepared by: Corporate Risk International
CRI Case No.: 07-32375

Table of Contents

1. Introduction

1.1. Predication

CRI was engaged by M.C. Dean to conduct research to determine if meaningful personal information may be obtained from open source websites to determine if social behavior, often referred to as social networking, may reflect personal information that may be deemed as unprofessional, unethical or unacceptable to an employer (government agency). Research also focused on the content of information posted on open websites or "chat rooms" to determine if sensitive or classified information has been posted or transmitted via an unauthorized communication source.

1.2 Description

CRI conducted research on names of 349 individuals or 'Test Cases' (herein after referred to as subjects). A variety of public record searches, detailed below, were conducted using all possible variations of subjects' names. Where possible, CRI obtained the e-mail addresses of subjects and performed same research using the subjects' e-mail address as search criteria. In certain circumstances, such as when subjects had very common names, CRI conducted basic research to identify past addresses of subjects so public record research and results could be limited to and analyzed in accordance with the geographic areas with which the subjects had current/prior footprints. To obtain this information, CRI utilized proprietary databases that contain addresses and identifying information on individuals. When listed on the consent forms, CRI used the social security numbers and dates of birth provided by the subjects' to access address history. After research was conducted, an Executive Summary and Report Form were completed for each of the 349 subjects. Subjects were randomly assigned a subject number and all identifying information was redacted from the Test Case Executive Summary and Report Forms. These results were submitted on June 10, 2009 under separate title 'Executive Summary and Report Forms Test Cases 001 - 349'.

2. Methodology

2.1. Description of research and search strings

CRI conducted the following open source/online database research on each of the 349 subjects:

2.1.1 **<u>Media Research</u>** - CRI conducted searches of multiple news media database sources, encompassing thousands of newspapers, trade journals, wire outlets located throughout the US and around the globe (English language only). When necessary, CRI incorporated the use of customized searches to quickly identify any adverse or pertinent mention in relation to the subject individuals.

2.1.2 **Internet/Open Source Research/Blog Research** - CRI conducted searches of Internet blogs, newsgroups, chat rooms, and websites for any adverse or pertinent mention of subject individuals. CRI utilized proprietary search methods and "crawling" search engines to access the desired information.

2.1.3 **Social Networking** – CRI searched the following social and professional networking sites which generally contain information self posted by the subjects. Many of these sites have security settings, which block certain information to the public, or limit viewing of results to others in the same 'geographic network', while others do not. CRI obtained login information for each of these social networking sites; however, due to expectations of privacy, CRI only accessed and searched for information that was readily available to any member of the general public searching for such information.

2.1.3.1 MySpace (www.myspace.com). MySpace is a social networking site that is geared to an international audience of individuals 14 years and older. Profile pages may consist of various types of information including name, date of birth, address, education, profession, etc. Pictures are often posted by individuals on the site. "Friends" of individuals often write messages to each other via MySpace. While many individuals do not place security settings for their MySpace pages, individuals are not easily searchable by first and last name. Rather, many people have their information linked to a nickname. Therefore, searches were conducted using subjects' true name, variations of their name, their email address (where available) and variations of their email address.

2.1.3.2 Facebook (www.facebook.com). Facebook is a social networking site that was started by a college student in February 2004. It began as a social networking site that was geared toward college students. It soon was expanded to high school students and then to the general public age 13 and older. Facebook profiles are similar to MySpace as they contain personal information regarding an individual, in addition to pictures, blogs, friend's comments/messages, etc. One generally needs to be a member to view profile information of individuals on Facebook, however, some individuals have "limited profiles" that are searchable via Google-type search engines. To be a member of Facebook, one must maintain a profile. Members of Facebook can set security settings to limit the viewing of their profile to only "friends" or for a particular "network" (city, region, school, etc).

2.1.3.3 Friendster (www.friendster.com). Friendster.com is a similar social networking site to MySpace in that it is geared to an international audience for individuals of any age. Profiles of individuals on Friendster are searchable via Google-type search engines or directly from the Friendster website without logging on. Individuals can limit their profile's access by applying security settings. Profiles are open to the public unless an individual applies security settings to limit the ability to view their profile.

2.1.3.4 LinkedIn (www.linkedin.com). LinkedIn is a professional networking site on which individuals list educational and professional credentials. Profiles are searchable via Google-type search engines, but a complete profile can only be viewed once logged into the website. An individual's profile also includes the names of individuals invited to be in their professional network.

2.1.3.5 Doostang (www.doostang.com). Doostang describes itself as an "online career community that connects people through personal relationships and affiliations." Members not only use Doostang to interact with one another, but also as a way to post jobs and recruit individuals. Members' profiles list educational and professional credentials. Members can also list their resumes and endorsements on the site.

2.1.3.6 KickStart (http://kickstart.yahoo.com). KickStart is a Yahoo! based professional networking site that was designed for college students, alumni, and professionals. KickStart profiles are searchable via Google-type search engines and contain educational and professional credentials. No sign-in is necessary to search profiles. ***Please note that this networking site was deactivated midway through this study.***

2.1.3.7 YouTube (www.youtube.com). YouTube is a public website where members can post video files. Searches are available through general Google-type search engines.

2.1.4 Global Compliance - CRI conducted searches of various open source databases comprising of numerous compliance, anti-money laundering, fraud and terrorism databases and are designed as a "Red Flag" search for all subject individuals. Specifically, these searches included:

- OFAC – SDN List; Bank of England; Terrorist Exclusion List; EU Consolidated List
- U.N Security Council List of Terrorist Associated Entities
- "Golden Chain" List
- Scandals Databases
- U.S. Government Agency Most Wanted Lists
- International Most Wanted Lists
- U.S. Regulatory Databases
- GSA Excluded Parties List
- Terrorism Database
- Independent Inquiry Committee Into the United Nations Oil-For-Food Program Report

2.2. Name matches

CRI was provided with consent forms which included subjects' names, dates of birth, social security numbers, and addresses. Due to lack of additional identifying or profile information, CRI returned numerous adverse 'name match' results. In an effort to reduce the reporting of such possible matches, CRI conducted research using subjects' social security numbers and/or dates of birth in an effort to obtain past addresses for the subject individual. In circumstances where a subject's name was found to be extremely common, searches and reporting of results were limited to the geographic areas that CRI was able to confirm to be associated with the subject. Please note however that address history obtainable by CRI is generally limited to a seven to ten year period.

CRI used a number of methods to rule out adverse or noteworthy information considered to be "name matches." For example, if adverse information was found for an individual with the same name as the subject, CRI looked at age and address history to determine if the information could likely be attributable to the subject. If the age and characteristics of the name match did not appear to match the age or demographics of the subject (i.e. by looking at a MySpace picture) CRI ruled out the adverse information as being attributed to the subject. Furthermore, if adverse information was found for an individual with the same name as the subject, but did not share any of the geographic or professional qualifications known to be attributable to the subject, this information was ruled out from the data set.

CRI relied on the experience of its researchers and senior management who have extensive experience conducting open source research to determine when noteworthy or adverse information could, with confidence, be attributable to the subject. This included verifying one or more pieces of data – such as matching addresses, ages, information posted by the subject on other forums – to confirm that the adverse or noteworthy information could, with confidence, be attributable to the subject. Experienced CRI researchers and management also used same criteria and good judgment when considering certain adverse or noteworthy findings to be name matches only. In many cases, the lack of additional demographic and background information about the subject and commonalities with jurisdictions did not allow us to rule out adverse information as name matches. In these cases, information was included in the data set. Since the type of information posted online varies from case to case, the ultimate criteria for determining whether or not the adverse information was a name match was the good judgment and experience of the researcher and management.

With additional background information, we are typically able to reduce the amount of name match findings.

2.3. Characterization of results

During the course of the research phase of this project, CRI maintained a data sheet used for recording results. For each search category described in section 2.1., CRI recorded the presence or absence of information as follows:

- No Information Found
- General Information Found
- Noteworthy Information Found
- Adverse Information Found

2.4. Definitions of categories

Prior to initiation of research, parameters for each characterization of results were established. The categories were defined based on the project objective to determine if unprofessional, unethical or information unacceptable to an employer (government agency) may have been posted on a public website. The classifications were also based on highlighting circumstances where sensitive or classified information was posted on a public forum.

To ensure categories were assessed equally for each subject, the characterization of results was limited to two experienced researchers. Characterization was then reviewed by a senior manager to ensure the information had been categorized objectively and accurately. Disputes over categorization were not prevalent and were resolved by joint review of the results by the researcher and senior management.

2.4.1. **Description of No Information Found** – No public reference to subject.

2.4.2. **Description of General Information Found** – Subject's name appears in public information, including media references and biographical information on corporate websites not posted by the subject. Information includes biographical information as posted on professional networking sites, such as LinkedIn.

2.4.3. **Description of Noteworthy** – Inadvertent or deliberate posting of personal information and/or inclusion of "questionable" material – i.e. possible underage drinking, profanity, extreme religious and/or political views on public forums. Also includes personal blog websites or photo websites that could be easily attributable to the subject. For example, the personal blog/website also includes information about the subject's professional career/employer or includes contact information or home address that would allow the subject to be easily contacted.

2.4.4. **Description of Adverse** – Deliberate and overly descriptive posting of personal and/or work related information on public forums. This includes information about the subject's specific work assignment, including listing descriptive information about colleagues and/or work site. Adverse classifications were also applied when references were found indicating illegal drug use or pictures appearing to show the subject engaging in illegal drug use.

2.5. Limitations

During the course of this research project, CRI encountered a number of limitations that, in our opinion, detracted from the efficacy of the study. These limitations are defined as follows:

2.5.1. **Limited information provided** – Lack of background information, such as a copy of subject's security clearance application, did not allow us to fully identify a number of subjects. It also hindered our ability to identify screen names and/or pseudonyms used by the subjects as their e-mail address or as their screen name on various websites. This limited our ability to identify potential noteworthy or adverse information.

2.5.2. **Name matches** – CRI encountered a number of name matches which limited our ability to analyze the true value of conducting open source research. However, if additional background information had been provided, CRI would have been able to rule out a number of name matches and thus obtain a more accurate picture of the extent of noteworthy and/or adverse information identified through open source research.

2.5.3. **Advance warning of research/signed consent form may have allowed applicants to remove questionable material** – Information on public forums, particularly on social networking sites, is easily deleted and/or edited. Thus, knowledge of this pending study may have resulted in a number of subjects removing questionable material which may be reposted at a later date.

2.5.4. **Lack of profile information provided did not allow for research to identify discrepancies and/or omissions from subjects' applications** – In our experience, one of the most valuable aspects of conducting public record research is to identify information that may have deliberately been omitted from an individual's resume, application or biographical history. It was not possible to identify these possible omissions because we were not able to compare subject's "public profile" with the profile supplied by the subject in his/her resume and/or application. If profile information had been provided, we would have been able to assign another characterization of results indicating where profile information was identified that was not included on the subject's application. This type of potential 'lead' information could be particularly useful for the adjudicator conducting the standard background check.

3. *Analysis*

3.1. Overall Analysis

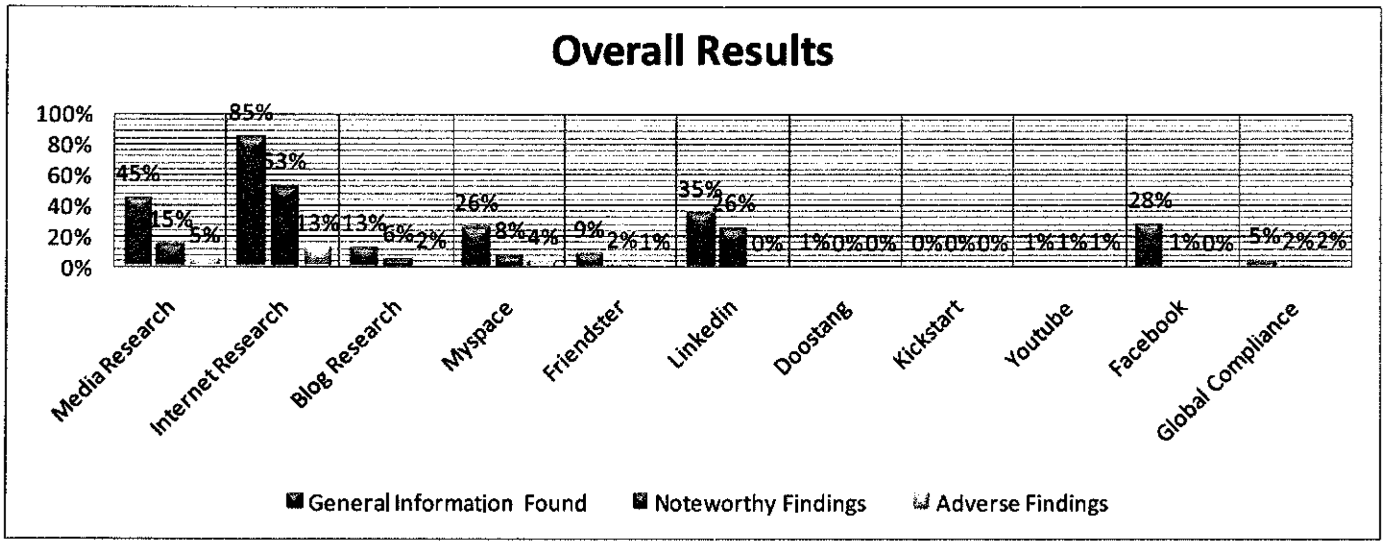
The following table demonstrates the overall results across each research category.

Based on review of the percentages in the following table, across all categories, Internet Research proved to be the search string that produced the most results. The top three categories for General Findings were through Internet Research (85% of subjects were found to be referenced in Internet searches), Media Research (45%) and LinkedIn (35%).

The categories that produced the most Noteworthy Findings also included Internet Research (Noteworthy findings were found for 53% of the subjects during internet research), LinkedIn (26%) and Media Research (15%).

The majority of the Adverse Findings were also found in Internet Research (Adverse information was found for 13% of the subjects through Internet Research) and Media Research (5%). However, the research category that produced the third largest percentage of Adverse Findings was MySpace (4%).

Internet research was defined as any information that could be accessed via 'Google' type search strings. Information that could be accessed through this type of search, such as MySpace pages and blog entries, were NOT captured in this result category, but were instead included in Blog Research and Social Networking Categories. Internet Research includes information posted on general websites and online media publications (but not those captured during searches of news media publications).



3.2. Search string analysis

As Indicated in the chart above, Internet research proved to be the search string that produced the most General, Noteworthy and Adverse results. Media Research produced the second highest amount of General and Adverse Results, while LinkedIn produced the second highest Noteworthy results. MySpace produced the third largest amount of Adverse results.

Doostang, KickStart, YouTube, and Global Compliance checks produced General, Noteworthy or Adverse results for 5% or less of the subjects. While Friendster produced results for 10% or less of subjects.

Based on the above findings, if open source research were to be limited to the top five most productive search strings, then CRI would recommend the following searches be conducted: Internet, Media Research, LinkedIn, MySpace/Facebook & Blog Research. Based on limited relevant findings, CRI recommends omitting the following search strings: Friendster, Doostang, KickStart, YouTube and Global Compliance.

3.3. Analysis of findings by age range

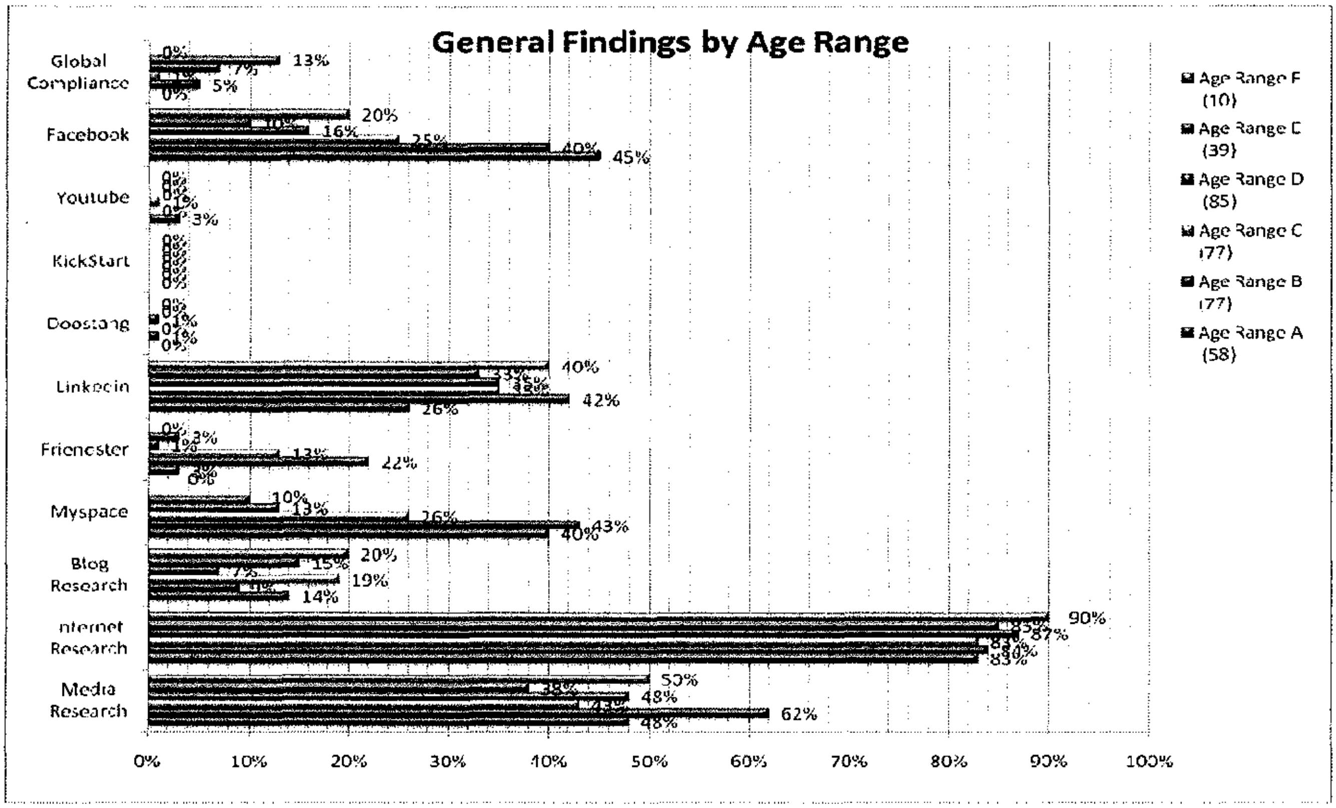
Research findings were also analyzed by age category to determine if open source research produced more Noteworthy or Adverse results among certain age groups. Within each age group, results for each search string were reviewed to determine if certain search strings produced more pertinent results within particular age groups.

At the initiation of the study each subject was assigned an age category based on the following criteria:

Age Range	Category	Number of Subjects
- age 18-24	A	58 subjects assigned
- age 25-34	B	77 subjects assigned
- age 35-44	C	77 subjects assigned
- age 45-54	D	85 subjects assigned
- age 55-64	E	39 subjects assigned
- age 65 +	F	10 subjects assigned
- n/a		3 subjects unable to qualify in above Parameters[1]

The following three charts demonstrate the percentages of General, Noteworthy and Adverse results by age ranges.

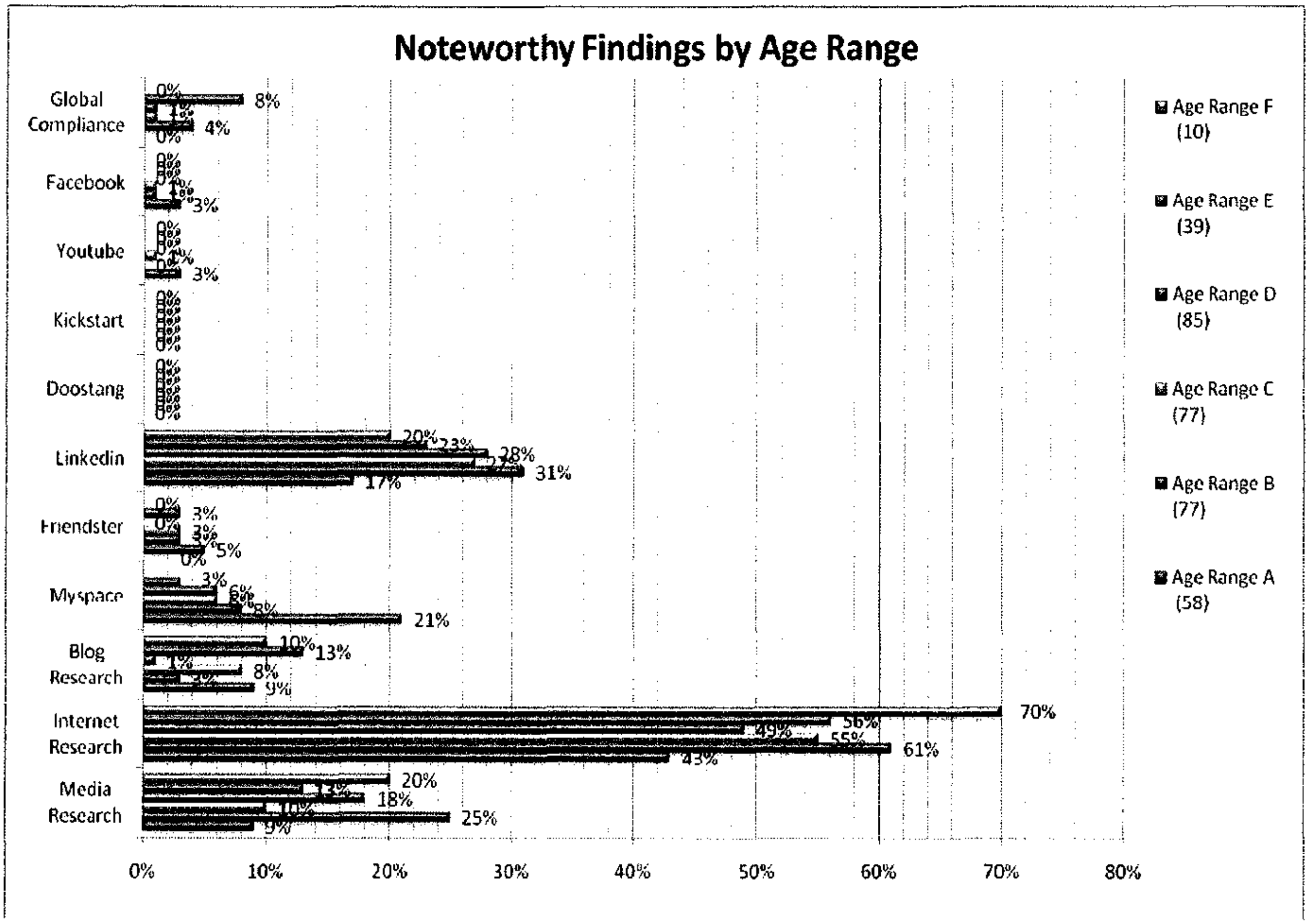
[1] *In two of the cases, the subject's did not list their date of birth, in the third case the subject incorrectly listed their year of birth as 2008.*



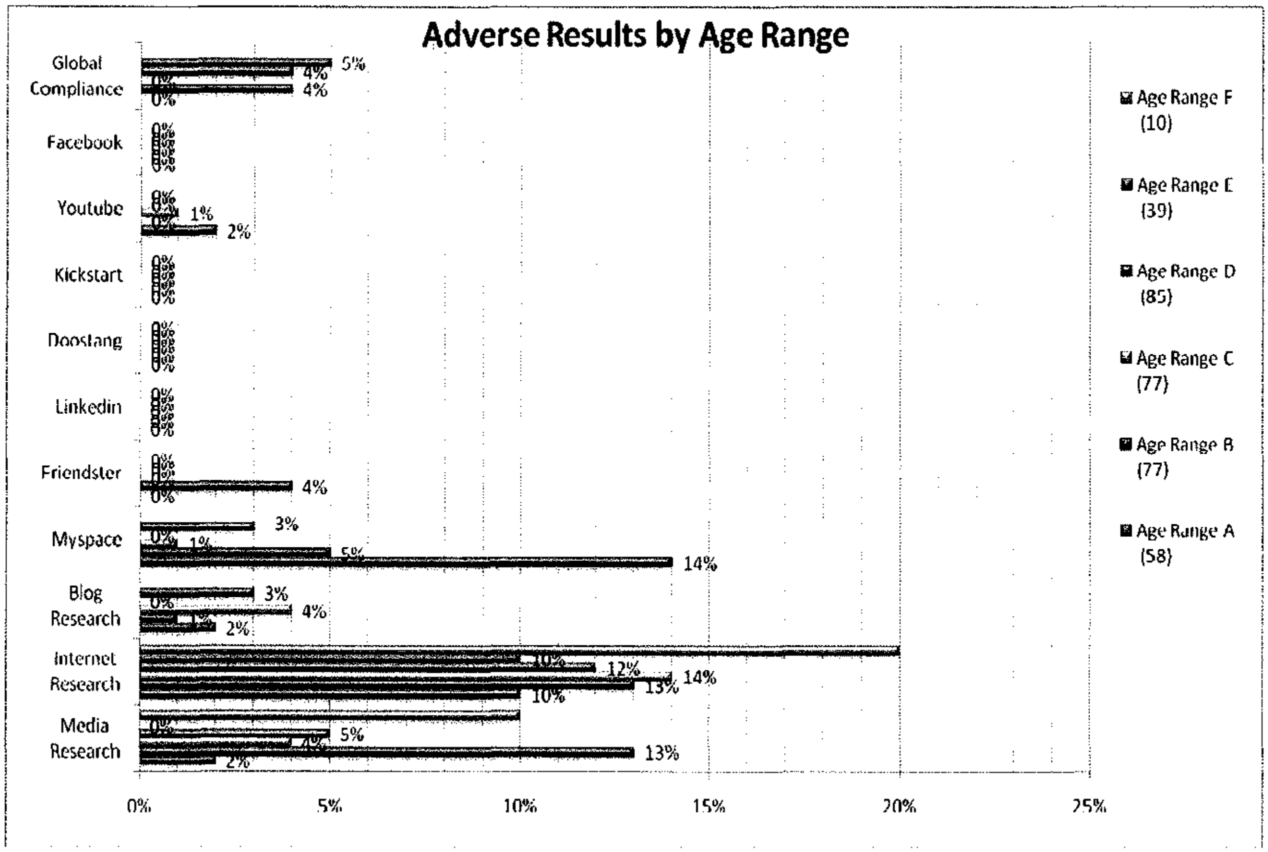
When reviewing the percentages of General Results across age ranges, there does not appear to be noteworthy differences across age ranges for Internet Research. General results were found during Internet Research for 80% or more of the subjects across age ranges. Media research produced General Results for 38 – 62% of the subjects across all age ranges. Blog Research was also fairly consistent across age ranges, with General Results being found for between 7-20% of subjects.

However, for Social Networking sites (MySpace, Friendster, and Facebook) the percentages of General Results generally decrease as a subject's age increases.

General Results were fairly consistent for professional networking site LinkedIn, with the lowest amount of findings in the youngest age category at 26% to the highest percent of findings, 42%, for subjects in the 25-34 age categories.



The same general pattern followed for Noteworthy Results. The percentage of findings for Media and Internet Research was fairly consistent across age ranges. Internet Research produced the highest percentage of results in Age category F, the highest age category, which also possessed the fewest amount of subjects (10 subjects). In all of the cases, the noteworthy findings pertained to the subjects' work history. The percentage of noteworthy findings during searches of Social Networking sites also decreased as a subject's age increased.



The percentage of Adverse Findings also remained fairly consistent across age ranges when conducting Media, Blog and Internet research. The highest percentage of Adverse Findings for research of Social Networking sites was in age group A (18 -24) year olds. It is worth noting however, that in age range E (55-64) adverse findings were found for 3% of the 39 subjects in this category, indicating that social networking research could still produce valuable results in higher age categories.

As noted earlier, the Adverse Findings category included deliberate and overly descriptive posting of personal and/or work related information on public forums. This includes information about the subject's specific work assignment, including listing descriptive information about colleagues and/or details on their specific work assignment. Adverse classifications were also applied when references to illegal drug use or pictures appearing to show the subject engaging in illegal drug use.

Based on review of subjects which received adverse categorizations across all research categories, approximately 13% percent of the adverse findings could be attributed to possible illegal activity. This included references to DUI convictions as well as references to or pictures of subjects engaging in illegal drug use.

The Adverse Findings sample was also reviewed to determine if there was any correlation of adverse information within subjects. Approximately 48% of the subjects which received Adverse classifications could be classified as having 2 or more pieces of adverse or noteworthy information attributed to them. However, due to the prevalence of name match findings, it is difficult to determine if the multiple pieces of adverse or noteworthy information can be attributable to the same subject or if one or more pieces of adverse information is a name match.

4. Key Findings

Review of specific findings for each of the 349 test cases identified five key areas where open source research could prove useful in the background review process. These five areas are outlined as follows:

4.1 Enhance profile information

Open source reviews, conducted of Media, Internet, Blog and Social/Professional Networking sites may allow for a more complete overview of a subject's background, activities, hobbies, etc. to assist the adjudicator conducting the background screening.

b6

[redacted]

4.2. Re-Investigation & Periodic Investigations

The relative ease and timeliness of conducting open source research could be useful for re-investigations and for periodic investigations on active clearance holders to determine if any key changes have occurred in subjects' lifestyle and/or activities.

In the following example, it was found that the subject maintained a personal business that was similar to the work he was doing on behalf of a government contractor. Depending on the nature of the work the subject is conducting, it may be important to look further into his personal business.

b6 [redacted]

4.3. Notify clearance holders

Often times, particularly for individuals who may be less Internet-savvy, an individual may wrongly believe that the information they have posted online, on a personal interest message board or on a social networking site, may not be easily traced back to the poster. As a result, they may inadvertently post information that could be of a sensitive nature. Open source research could allow adjudicators to alert active clearance of holders of possible sensitive information online, which they could then remove.

b6 [redacted]

This level of detail, particularly the descriptive pictures of the subject's housing during her posting in Israel could be a security concern. The subject could be encouraged to make her photo website password protected.

4.4. Identify friends and business associates through networking sites for field interviews

Social and professional networking sites, i.e. MySpace and LinkedIn, generally include detailed information about the subject, but also include the names, and in some cases, the contact information for friends and current and past business associates, all of which is posted publicly.

This could allow for easy identification of friends and associates not listed on the subject's application to be contacted for interviews.

4.5. Identify issues or concerns not developed during the standard clearance process

In certain circumstances, significant adverse information could be found during open source research that was not uncovered during the standard clearance process.

b6 [redacted]

b6 [redacted]

5. Recommendations

5.1. Identify sites most useful for conducting open source research

Based on review of specific test case findings and general analysis of results across age categories, CRI recommends that the following types of open source research be conducted on clearance applicants across all age ranges:

Media Research
Internet Research
Blog Research
Social Networking – MySpace, Facebook
Professional Networking – LinkedIn

In addition, since the inception of this project, the social networking/micro-blogging site "Twitter" has reportedly become the fastest growing social networking site and the third most used social networking site along with Facebook and MySpace. Twitter is a social networking and micro-blogging service that enables its users to send and read other users' updates known as tweets. Tweets are text-based posts of up to 140 characters in length. Updates are displayed on the user's profile page and delivered to other users who have signed up to receive them. Twitter users can enable privacy restrictions similar to those possible on Facebook and MySpace. However, if the user does not make their profile private, it is visible to the general public and does not require the searcher to login (as one must with Facebook). Twitter also appears to be frequently utilized by members of the professional community. For example, the Mayor of London maintains a public twitter profile. However, Twitter also allows its users to maintain their pages under pseudonyms, which could make searching more difficult. Nevertheless, due to its growing popularity, it should be considered for possible inclusion in future studies.

5.2. Supply profiles/applications to Open Source vendor

Supplying the entity conducting the open source research with the subject's application will greatly enhance the relevance of open source findings. Information on the subject's address history, e-mail addresses, education, past employment and professional credentials would allow the researcher to conduct more focused searches, which is particularly helpful when researching subject's with common names. For subjects with extremely common names, conducting searches using the subject's name and known identifying details could also allow for identification of results that may not otherwise be captured due to the extensive volume of results for subjects with common names. Complete profile information will allow the researcher to rule out the majority of name matches and will also allow them to identify possible omissions from the subject's application or resume.

5.3. Open Source Research as first step in clearance process

Conducting open source research prior to the formal clearance process will provide the adjudicator with a comprehensive public profile on the subject, giving the adjudicator greater familiarity with the subject allowing the adjudicator to focus the inquiry in a more useful fashion. Any red flags developed during the open source process could also be more easily addressed during the formal clearance process. The adjudicator could also be provided with a list of contacts for potential interview that were not listed by the subject on their application.

5.4. Incorporation into standard clearance process due to affordability/quick turnaround

Open source research can generally be conducted within a 2-5 business day turnaround time. Fees are also extremely competitive. In certain cases, identification of significant red flags (that could results in rejection of a clearance) could be identified at the outset of the investigation, thereby reducing the overall length of the clearance investigation and, as a result, also reducing costs.

A trained and experienced open source researcher with access to the appropriate search tools and research techniques could produce an open source profile on a subject in 2 -5 business days or less. However, the formal and on the job training required to develop the level of research skills necessary for this type of assignment can take approximately 6 months to a year. CRI maintains a training program during which researchers receive formal training, which generally takes 2-4 weeks, and is followed by the researcher being paired with a senior researcher who provides mentoring over the course of the following six months. CRI estimates that it can take approximately 6 months to 1 year for a researcher to develop the skill level necessary for this type of assignment. Furthermore, each researcher is trained to utilize CRI's proprietary research tools and techniques designed to identify the most pertinent findings and rule out name match information. Although CRI's researchers come from a variety of professional and academic backgrounds, the best researchers (i.e. those who are able to develop the most creative searches and produce the most pertinent findings) tend to be individuals who are extremely comfortable and experienced with using the Internet in their personal and academic lives.

Furthermore, the sites and resources through which open source research can be conducted are constantly evolving, indicated by the growth of Twitter during the course of this project. The researcher would need to be up to date on all of the new websites, techniques and resources to access during open source research. CRI maintains a research team dedicated to indentifying new resources for conducting open source research.

Although the cost per subject can vary greatly based on volume, information provided, and necessary turnaround time, please see the following cost model for conducting open source research in line with the requirements of this study. However, the following cost model assumes that CRI would be provided with the full background details on the subject – i.e. a copy of their resume and security clearance application. Reports could be turned around as they are completed in approximately 2-5 business days per subject or could be provided in batch reports, i.e. 200 reports submitted per month. A report similar to the Test Case report would be submitted for each subject:

Number of Subjects (reviewed per year)	Fee Per Subject
0 – 100	$650
101 – 500	$550
501 - 1000	$450
1001 – 2000+	$375

5.5. Open Source research becoming a standard in Industry

Likely for many of the reasons outlined above, conducting open source research is becoming a standard during pre-employment inquiries and other employee/client vetting processes. For example, a March 29, 2007 media article published in The Plain Dealer details a recent college graduate applicant who withdrew his employment application due to pictures on his MySpace page. Researchers found what "looked like a 32-ounce glass of beer in his hands" and commentary on "how smashed he got at a recent party and references to the fact that they were smoking marijuana at the party." A May 29, 2007 media article in The Boston Globe details an applicant at a consulting firm having a MySpace page with pictures of the applicant Jell-O-wrestling. As one employer is quoted as saying in this article, "When you're comparing two or three people, everything matters." Countless other media articles discuss similar experiences of recent college graduates due to compromising pictures and comments posted on social networking websites.

A November 14, 2008 article from Computerworld reported that President Barack Obama's transition team asked applicants for jobs in the new administration to provide links to blog posts and social networking profile pages that could embarrass Obama. Even on individual profiles that are restricted on Facebook and MySpace, individuals conducting due diligence inquiries are for the most part still able to learn if an individual in question maintains a profile, depending on the commonness of the subject's name, and at least see the subject's "profile" picture. Some individuals have been known to have profile pictures showing questionable or even illegal acts, such as pictures of illegal drug use.

Although they may not be as frequent users as individuals in the 18 – 34 age ranges, open source research on individuals across all age and skill levels is still recommended. More seasoned employees including senior executives have been known to maintain Internet profiles that may be considered damaging to a company's reputation or counter to its company culture. In addition to Internet profiles containing damaging reputational information, these profiles can also contain proprietary information. In January 2005 Mark Jen, a former Microsoft and IBM employee, was hired by Google and began recording his impressions of his new employer, including criticism, in his blog, Ninetyninezeros. Eleven days after being hired by Google, Jen was fired for his blogging activity. Some media and Internet sources claim that Jen was fired for distributing Google trade secrets; however, Jen has stated that he only blogged about Google's new employee orientation procedure and removed the inappropriate content before he was fired.

In another example, in 2003, Microsoft Corporation contractor Michael Hanscom was fired after posting pictures online of computers from Microsoft's rival Apple arriving at a Microsoft loading dock. Microsoft claimed that since Hanscom described a building in his online posting he violated security.

6. Appendix

6.1. Definitions of Terms used in Report

Adjudicator – Refers to individual(s) who would be conducting the security clearance process as it exists today.

Name Match – Refers to cases where the matches were found for individuals with the same full or partial name as the subject. Due to the commonality of the subject's name and lack of additional identifying information provided by the subject, the researcher was unable to confirm if the adverse or noteworthy information did in fact pertain to the subject.

Open Source Research – Refers to research conducted as part of this study, including review of Media, Internet, Blog, Social/Professional Networking Sites and Global Compliance Databases.

Researcher – Individual conducting the open source research.

Security Clearance Process – Refers to existing clearance review process that does not include open source research.

Subject (or Test Cases) – Refers to the 349 individuals on which open source research was conducted.

END REPORT

Corporate Risk International

Headquarters
11440 Commerce Park Drive
Suite 501
Reston, VA 20191
T: +1 (703) 860-0190

Houston
9595 Six Pines
Bldg 8, Level 2, Suite 8210
The Woodlands, TX 77380
T: 832-217-0313

London
Corporate Risk International Ltd.
48-49 Russell Square
London WC1B 4JP
T: + 44 (0) 207-612-1970

www.corprisk.com