(S//SI) Job Vacancy: More Than a Mission...A Challenge!

FROM: Data Acquisition (S3)

Run Date: 01/08/2004

FROM: Data Acquisition (S3)

(S) The Iraq Survey Group (ISG), led by CIA and DIA, is responsible for the Document Exploitation (DOCEX) mission within Iraq. DOCEX includes tons of physical documentation that is being collected throughout Iraq, physical media confiscated, as well as interrogations. This vacancy is for the computer media exploitation support to the DOCEX mission. NSA has agreed to continue to staff this vital mission by deploying three computer media exploiters for 120-day increments.

(S) A team of three will deploy early calendar year 04 and then be replaced by a new team of three. The main computer media and document exploitation mission is accomplished at Camp Doha in Qatar. There is a possibility that a selectee may have the opportunity to work in Baghdad; however, the focus will be in Qatar.

Duties: (S) The ISG has three major focuses - WMD, Counterterrorism, and locating any information associated with Capt Speicher (POW from first Gulf War). While the ISG does not have a SIGINT mission, the presence of NSA expertise and ability to reach back for support has proven very valuable - both to the ISG's mission as well as NSA's mission.

(S) The applicants for this position will:

- create images of standard PC hard disks using standard forensic copy tools such as DCFLDD and SOLO II disk copiers.
- use basic computer forensic tools to conduct text searches of disk drives from standard PC systems.
- extract data from digital tape media using both off the shelf tools and Linux-based utilities.
- conduct searches of media for non-overt file information using advanced forensics tools such as iLook, FTK Toolkit.
- perform target analysis to include trying to identify key foreign facility personnel to target for HUMINT exploitation in support of technical exploitation.
- conduct basic data extraction from non-PC data sources such as PDAs, GPS units, building security systems, and voice mail systems.
- create simple shell or Perl scripts under Linux for data extraction and search purposes.
- use VMWare or similar virtual machine "sandbox" technology to view object-oriented data in its native environment.
- develop software and hardware-based exploitation tools on an as-needed basis to support collection and analysis operations using Linux.

- (S//SI) interface with external entities such as CIA or DIA to identify systems remaining in use that should be targets of ongoing technical collection operations.

QUALIFICATIONS/EXPERIENCE: (S//SI) Applicants should possess the following skills: A Unix (Linux preferred) background, significant knowledge of Microsoft based systems, some scripting ability (Perl preferred), talent for analysis. Knowledge in the following areas are highly beneficial, but not required: computer forensics, working with large data set, web programming, intrusion analysis, computer system vulnerabilities, system administration, databases, intelligence analysis.

TRAINING REQUIRED: (U) All selectees will be provided training in the SIGINT Forensics Computer Lab prior to deployment. Level of on-the-job training will be assessed per individual needs. Additionally, selectees are required to attend a one-week preparation class that is

CENTCOM approved and held at a Ft. Bliss Texas.

EMERGENCY ESSENTIAL: No
POSITION TITLE (WORK ROLE): Global Network Exploitation Analyst
MANAGEMENT LEVEL: non-supervisory
SKILL COMMUNITY: Computer Scientist
ALTERNATE/RELATED SKILL COMMUNITIES: Networking and Telecommunication
FUNCTIONAL TITLE: Data Forensics Analyst
EMPLOYMENT CATEGORY: Full Time
DAWIA: No
GRADE: Grade 11-13
LOCATION: Camp Doha, Qatar
REPORT DATE: ASAP
PHYSICAL REQ: No
LENGTH OF TOUR: 120 days
SOCIAL RESPONSIBILITIES: No
INFO ON POSITION: [redacted] Chief S3115, [redacted]
SELECTION OFFICIAL: [redacted] Chief S3115, [redacted]

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108