ACBI News

The ACBI News is published quarterly for the membership of the Association of Certified Background Investigators (ACBI), a section (c)(6) not-for-profit organization. Unless otherwise attributed in writing, all content of ACBI News is provided by and for the membership of ACBI, and does not reflect the official policies or opinions of any governmental agency or commercial entity.

Inside This Issue

President's Message

The remarks this time will be short and related to the ACBI elections, sorry no Presidential or VP debates have been scheduled which I'm sure you will appreciate.

The ACBI board has been re-writing the bylaws and making changes to realign the terms of the officers and board members to make them match up better with our national conferences. The VP has normally been the spearhead of the conference, working for a year on the setup but was not the VP, except if re-elected, for the conference year. With the realignment this will change and we will have some one-time three-year terms.

With that being said, a committee will be setup in November to seek volunteers and or nominees for the following officers: President, Treasurer, Secretary, and one Board member. The President will be a one-time three-year term. Exact details will be provided during the election period. We currently have an appointed Assistant Treasurer, Jorge Garcia, highly qualified, who will run for and hopefully take over the

Treasurer's position. A new VP, Diane Griffin, has recently been appointed since the resignation of our former VP, Bob Nesvick. Now we need people to step up to serve as President, Secretary and Board member. The Board member is an easy position and a good way to work your way into the organization. The Secretary's job has been made much easier with the new website, and many of the duties have been automated. The same can be said for the position of Treasurer. Now for the easiest job of all – the President. All you need to do is to care about the organization and its principles, get good people on your board and then get out of their way and let them do their job. Well, it's not quite that easy, but almost.

This is your organization. Get involved and be more than a name on a roster. ACBI has come a long way since its inception in 2002. ACBI has accomplished many things and has an excellent reputation with the agencies and contract companies. Each group of ACBI officers has pushed the organization forward, but there are many more things that we can do that are still unfinished. We need your help. Please consider running for a position on the ACBI Board. We could also use members to work on committees, as liaison contacts, researchers, etc. If you have a talent and want to be more involved, please raise your hand, I can guarantee that you will greeted with open arms.

Sincerely,

Robert A. Kuropkat, President ACBI
We have met the enemy and they are "US"! (POGO)

Meet ACBI's Vice President

Diane Griffin is the Founder & CEO of Security First & Associates, and has over 20 years of experience in Defense and Intelligence industries where she held progressive security, leadership and management roles with small to large defense contractors. In her consulting practice, Diane has teamed with other consultants to provide security support to small and midsize defense contractors. Besides the duties of a security consultant, Diane also is a credentialed Background Investigator, assisting various contractors with background investigations.

Diane is an active member in several security organizations (ASIS, ISACA, and ISWIG.) She is Chairperson of the NCMS Chesapeake Bay Chapter 26. She is also the author of several security articles and eBooks. Diane is very active with community services organizations who give back to our community through programs of positive impact for all such as "Secure the Call," which provides donated cell phones to domestic violence

victims; and the organization "Make a Change," which provides donated book bags and teddy bears to children in the foster care system.

Diane received her B.S. degree in Organizational Management from Colorado Christian University and a MBA from University of Phoenix. Diane considers it a privilege to be involved with ACBI and hopes to continue to be a partner and contributor in helping to shape and improve national security policy and direction.

Feature Article: Visa Fraud

Visa fraud is a continuing problem; however, the types of fraud being committed have adapted over time as old schemes are discovered and perpetrators share information about control weaknesses and new tactics that are effective. The most common schemes today continue to be submitting false documentation for a temporary visa (temporary worker - H1, students - F1, summer work and travel - J1) that disguises their intention to immigrate illegally (overstay their visa). Some fraud scheme examples are: phony companies sponsoring H (worker) visas; falsifying proficiency in English for F (academic) or M (vocational) student visas; or exploiting the applicant by placing them in a different job for J (exchange) visas under the summer work and travel program.

To help combat this fraud, the Department of State employs Fraud Prevention Managers (FPM) at foreign posts. The FPM's are assisted by domestic staff with knowledge of local customs and contacts. One would assume that the ideal solution to a problem is to have the right people in the right place with the right tools. But according to GAO Report 12-888 the U.S. Department of State has found a way to thwart each part of this solution. For example: 1) Have they assigned the right people? As of April 2012, about 81% of FPM's were entry-level or non-specified grade employees. 2) Are they placing them in the right place? As of April 2012, 84% of FPM's were either part-time or rotational (on the job about 6 months). Since the FPM's are part-time, they rely on their domestic staff to identify fraud. What could possibly go wrong here? And they rely on US-based support to investigate fraud. 3) Do they have the right tools? Most of the foreign posts didn't use the Kentucky Consular Center in Williamsburg KY, which was established in 2000 for administering the Diversity Lottery Program. The KCC also can relieve the fraud workload overseas especially in the H-1B and J-1 summer work and travel visas (SWT), if asked. Most FPM's didn't even know how to ask KCC for help. There also are classroom and on-line training courses on fraud prevention, but the Department of State doesn't require the FPM's to take these courses and doesn't even track whether they have been trained at all. So, the FPM's are not receiving the training that could benefit them (and this is distance learning), and

even when they are trained they take their experience and training with them when they rotate to their next job.

There are back-up systems in place but they generally address the problem after the applicant is in the US. Diplomatic Security Service (DSS) will investigate criminal networks within the US. ICE will investigate benefit fraud. CBP has the authority to deny entry into the US. And USCIS conducts site visits and administrative inquiries. (Note: Former ACBI President Ed Kassof has worked the ICE contract for many years. As of FY2013, CSC is the only ICE contractor and work is concentrated geographically. Members can contact Ed directly at kassof9464@satx.rr.com about the ICE contract.)

Visa fraud has grown in size and sophistication since visa applications have increased dramatically since 2003. And the current administration directed the State Department in January 2012 to increase visa capacity for China and Brazil by 40% and expand the visa waiver program in order to "create jobs and spur economic growth" (see EO 13597 and the 180-day progress report.) The GAO Report 12-888 described China and Brazil as among countries (along with India, Mexico and the Dominican Republic) that accounted for the majority of confirmed fraudulent visa applications in 2010. The bottom line is the US Government strongly encourages the issuance of visas and they want it done as quickly and painlessly as possible to satisfy all the stakeholders (schools, businesses, travel & tourism industry, immigration advocates, etc.)

The problem of enforcing the H-1B visa program is challenging, as evidenced by this OIG-DHS Report published in August 2011. The report documents another example of available fraud training not being given to the people responsible for detecting and adjudicating fraud (see above GAO report, pages 29-31). At the two ICE centers in Vermont and California, 71% of the ISO's (Immigration Service Officer) had not taken the fraud course on H and L visas. And 58% of the ISO's had not taken the fraud training for H-1B and H-2B visas. Remember the goal? The right people, in the right place, with the right tools?

This OIG-DHS report came after testimony was presented to the Senate Judiciary Subcommittee for Immigration, Refugees and Border Security on July 26, 2011. During that hearing, a written statement was submitted by a whistleblower on how a foreign IT company was using B-1 visas to bypass the reduction of available H-1B visas. H-1B visas are issued for technical work that requires a bachelor's degree or equivalent training. The amount of H-1B visas issued to foreign workers is capped, and the employing companies must pay a minimum of $65,000 in annual salary and withhold US taxes. B-1 visas, on the other hand, are used for temporary visits (training, conferences, etc.) and there are no rules on salaries. Thus, these B-1 visitors were

allegedly assigned to positions in the US and being paid their home country salaries – about $15,000 a year. They started to complain to their HR representatives after learning that their foreign salaries fell short of the cost of living in the US. In addition, their employer was not paying US taxes, but was billing their US clients for fully paid H-1B positions. If the allegations are true, this is what is known as exploitation. (Note: The whistleblower's civil suit against his employer was dismissed in August 2012 in Alabama state court; however, the suit did not address visa fraud allegations. A federal investigation into visa fraud continues into what is undoubtedly a very complex case.)

E-Verify and the I-9: An Overview

The E-Verify employee verification system was introduced after passage of the Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) of 1996. This web-based system compares information on the I-9 Form, which all employers must complete, with data maintained by the Social Security Administration (SSA) and Department of Homeland Security (DHS). Participation in the E-Verify program is free and voluntary for most employers; however, federal employers and federal contractors must participate. In addition, some states require employers to participate. E-Verify queries must be sent in within three days of a newly hired person starting work. The E-Verify system cannot be used to pre-screen applicants. As of October 2012, there were 404,000 employers using E-Verify in the U.S.

On the I-9 Form (Employment Eligibility Verification), which must be completed for all new hires after November 6, 1986, and working in the U.S., Section 1 is completed by the employee or their translator. Section 1 lists name, address, DOB and citizenship status. Providing a SSN is optional for some reason. Section 2 is completed by the employer and is used to verify which type of identification documents were produced to establish the new hire's identity and employment authorization.

E-Verify is an improvement over the paper-based I-9 verification system because falsified documents can convince an employer that either doesn't know what makes a document genuine or is not familiar with documents from another state or country. Before E-Verify, the employer only had to attest that the documents appeared to be genuine. Employers seem to like it since it is fast, free, 99.5% accurate; and it is cheaper than submitting to an I-9 audit by USCIS.

So, what could possibly be the reason why E-Verify is not required for all employers? Let's read GAO Report 11-146 of December 17, 2010, to learn what some of the problems are. A mismatch of the spelling of names, much more common in foreign-born employees, on the source documents can generate a TNC (tentative non-

confirmation). Also, a nick-name, name change or hyphenated last name that is recorded differently on the source documents. Identity theft by the employee is another way around E-Verify. How about intentional fraud by the employer? Another reason is the time it takes for TNC workers to clear up the problem, which could entail filing a FOIA request that takes an average of 104 days to fulfill. What if your employer had you standing by for that long and you really needed the money?

Real ID Act Security Challenges

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 required the Social Security Administration (SSA) and Department of Homeland Security (DHS) to coordinate ways to improve the security of the SSN account card. The Real ID Act was passed by Congress in 2005 to set minimum security standards for state issued driver's licenses or personal ID cards. The date for enforcement has been pushed to 2013.

Consider the lowly Social Security Number (SSN) account card, which was introduced in 1935 as a means to track employee retirement, survivor and disability benefits; and never intended to positively identify the cardholder. By law (starting in 1983) the card must be made of bank note paper, but there are 50 different valid versions of the car in use today. Prior to 1978, applicants did not even have to provide proof of age or work eligibility. Yet the SSA card is the KEY document used by DHS to verify authorization to work! The reason this should concern you is that both the GAO and the OIG-HHS conducted investigations by applying for SSN's using counterfeit birth certificates for fictitious children. Their fictitious applications were approved.

According to GAO Report 06-303 of March 2006, which looked at the progress SSA was making with DHS, a few solutions were proposed for improving SSN card security: better paper; plastic machine readable cards; biometric ID on cards; or doing away with the cards completely and just issuing SSN's. It will take some bold leadership and funding to achieve more than the minimum required by law.

Skip ahead to September 2012 and GAO Report 12-893 is released. With only a few months to go before the Real ID Act of 2005 is to be rolled out nationally, we have made the following progress. All states now check driver's license applications with SSA (via SSOLV – Social Security Online Verification) to verify the authenticity of the applicant; and 42 states check with DHS (via SAVE – Systematic Alien Verification for Entitlements) to determine non-citizen's immigration status. Because of the SSA verification, the number of fraudulent driver's license applications using a bogus SSN has decreased. Another tool being used effectively by some states is facial recognition software, which detects whether the applicant already has a license in another name.

Challenges still remain the area of cross-state license applications (fraudulently obtained driver's license from one state used to get a license in another state.) At present, the only way to check a license number in all 50 states is via a state-by-state NLETS query which is only available to law enforcement personnel. What to do about fraudulent birth certificates remains a problem since ID theft is more common than bogus documents. In 15 states, the vital statistics bureaus have no restrictions on who may receive a genuine birth certificate. Currently, there are thousands of versions in use. Remember IRTPA? The Act required DHS to issue guidance and funding to the states to improve the security features of their birth certificates. Over $260 million has been provided to the states through federal grants from FY2008 to 2011, but final DHS rules have not yet been published. If a state decides not to comply, then TSA could refuse to honor a license/ID card from that state for travel purposes.

Contract Investigator Help

Seven of the current BI contractors were contacted last month and requested to send information about contract BI work available in FY2013, which started on October 1, 2012. As of press time, two of the contractors -- Omnisec and MSM Security – have responded. Their information is shown below:

OMNISEC: We currently have multiple contracts under DHS and in the Intelligence Community. There is the potential for a new contract for FY 2013. Our recruiter point of contact for Investigations (credentialed, or non-credentialed) is Tiffany Black, who can be contacted at (703) 652-3438, or tblack@omniplex.com .

The Special qualifications for the BI applicants that we are looking for are: Minimum of three years experience conducting general investigations as a local, state, military or federal law enforcement agent OR must have current credentials for three years to conduct background investigations for U.S. Government security clearances, four year degree, and have completed an approved investigator training program. Applicants must be able to pass a U.S. Government background investigation for required clearance. Additionally we are seeking Contract Investigators with Full Scope Poly or willing to sit for a polygraph exam (Washington DC; Baltimore MD).

We are currently recruiting in the following geographic locations: Northern VA; Baltimore MD (Fort Meade); Anchorage AK; Montgomery AL; Little Rock AR; Sierra Vista/Douglas/Tucson AZ; Lompoc CA; Los Angeles CA; Monterey CA; San Francisco CA; San Luis Obispo CA; Riverside CA; Rosamond CA; Colorado: Buckley AFB; Denver CO; Washington DC Metro; Orlando FL; Augusta GA; Hawaii; Shreveport LA;

Bedford MA; Minneapolis MN; Oxford MS; Starkville MS; Greensboro NC; Raleigh NC; Las Vegas NV; Omaha NE; Minot ND; Albuquerque NM; Las Cruces NM; Rochester NE; New York NY; Cincinnati OH; Dayton OH; State College PA; Pittsburg PA; Puerto Rico; Knoxville TN; Memphis TN; Laredo TX; El Paso TX; Del Rio TX; San Antonio TX; San Angelo TX; Salt Lake City UT (also Camp Williams UT area); and Harrisonburg VA.

MSM Security: For FY 2013, MSM Security Services, LLC will continue to perform the following US Government contracts:

Customs and Border Protection (CBP): Three years experience as a Federal Background Investigator or equivalent required.
Department of Homeland Security (DHS): Three years experience as a Federal Background Investigator or equivalent required.
Office of Personnel Management (OPM): Must currently hold OPM Credentials or have conducted Federal Background Investigations within the last 18 months. Positions are located within 100 miles radius of the Washington, DC Metropolitan area.
Equal employment opportunity (EEO): Require current certification as an EEO Investigator.
Securities and Exchange Commission (SEC): Experience as a Federal Background Investigator.

Minimum Qualifications: Other than OPM position identified above applicants will qualify with three years of previous investigative experience as a Federal, State or Local Law Enforcement Investigator or Military Investigator (i.e. federal agent 1811, military investigator 97B, detective, probation officer or state investigator). Intermediate typing and computer skills are required and U.S. citizenship. Due to the nature of this position, a valid driver's license and transportation are required. Must have excellent writing and communication skills and have the ability to deal with various types of individuals. Occasional travel may be required.

Applicants should hold an active Top Secret clearance or have a favorably adjudicated SSBI. Those applying without a Top Secret clearance will be considered based on workload of the area they reside, and must be able to pass a single scope background investigation (credit, criminal, civil, employment, mental health/medical).

Center for Medicaid and Medicare Services/Health and Human Services (HHS): Ability to use Smartphone technology is a must for the position of Fraud Prevention Inspector. A security clearance is not required but applicants must pass a background check.

To apply for any of these positions, please submit your resume to: jobs@msmsecurity.com. For questions regarding this position, please contact Angelica Rutherford, Recruiting Manager, at arutherford@msmsecurity.com or Jim Wright, Senior Recruiter, at jwright@msmsecurity.com.

Productivity Tip: When conducting a background investigation that requires testimony of neighbors (i.e. the OPM "RESI" item), help yourself and other BI workers secure these hard-to-contact sources. Advise the subject that you will be contacting neighbors and ask that he notify them that you will be in the neighborhood in the future. If you know the approximate dates, provide that as well. The investigation should come as no surprise to the subject or his immediate neighbors, and this could help persuade those that would otherwise be intimidated by strangers flashing a badge and asking personal questions. This is needed in areas other than near military bases or Washington DC.

Security Tip: Making photo copies of your federally-issued credentials is a misdemeanor violation of federal law. Title 18, United States Code, Section 701 reads:

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both"

So, don't allow a school or employer to copy your credentials as a quick proof of an inquiry unless they can show you a federal law that supersedes this one. Never relinquish control of your credentials. They have their rules and we have ours.

Helpful Links

ACBI members should learn about the history, structure and mission of the federal agencies and departments they serve. The more you know about these federal clients, the better prepared you will be at predicting the direction of BI work, and you might even help them achieve their goals by submitting a

beneficial suggestion. Here are some public website links to federal clients you may work for directly or indirectly:

Office of Personnel Management (Federal Investigative Services)
U.S. Courts (District, Bankruptcy, PACER)
U.S. Department of Veterans Affairs
U.S. Department of Commerce
U.S. Department of Energy
U.S. Department of Education
U.S. Department of Health and Human Services
U.S. Department of Housing and Urban Development
U.S. Department of Justice
- Office of the U.S. Attorney
- Bureau of Alcohol, Tobacco and Firearms
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marshals Service
- National Security Division

U.S. Department of Labor
U.S. Department of State
U.S Department of the Treasury
U.S. Department of the Interior
U.S. Department of Defense
U.S. Department of Homeland Security
- Customs and Border Protection
- Citizenship and Immigration Services
- Immigration and Customs Enforcement

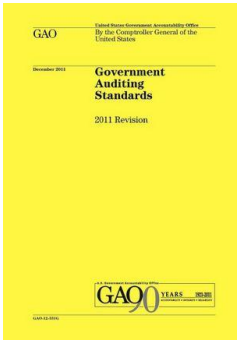
National Security Agency (NSA)
National Aeronautics and Space Administration (NASA)
Director of National Intelligence (DNI)
Social Security Administration (SSA)

Reports of Audits and Investigations: Don't laugh. You're too busy for homework? You can increase your value as a BI worker by staying informed about your federal clients. One way to do this is to read public reports about their programs, problem areas and possible solutions. Here are two ways to find these reports:

Office of the Inspector General (portal to all federal OIGs). All federal departments and most agencies are required by law to have an independent office of inspector general (OIG) that reports semi-annually to the Congress. The OIG mission is to prevent fraud,

waste, and abuse in the programs that their respective department/agency administers. The OIG typically has a criminal investigation group and an audit group. The audit reports are public, as are their semi-annual reports to Congress. Once you understand the jargon and can get past the boilerplate wording, some of these reports can make interesting reading if they affect national security or other related BI work. Do not be intimidated by these reports! The auditors are required to follow the Government Auditing Standards (AKA "the Yellow Book") and will report a finding in this format:

Criteria:	What regulation, law or policy should be followed?
Condition:	What is actually happening that violates the criteria?
Cause:	Why is the condition happening?
Effect:	What is the condition costing us in terms of money, hours, etc.?



After this, the OIG will make a recommendation that should correct the condition. This recommendation is directed to the most senior official that has the authority to take corrective action. The department/agency can either concur or not concur with the recommendation. If they concur, there is a timeline for corrective action established so that the condition does not repeat. In some subjects, such as financial reporting for the Department of Defense, there have been repeat findings going back for decades. The issue of independence continues to be debated. The OIG employees are federal employees and are paid a salary by their parent organization. The independence comes from their reporting to Congress. But it is a rare auditor (in the public or private sector) who will stand up to his employer by publishing an embarrassing report. That's why we will continue to have scandals for as long as there are human beings trying to earn a living by getting around some regulation.

Government Accountability Office (GAO) GAO works for Congress and investigates problems when someone in Congress needs comprehensive proof that a federal program is not working. The GAO report will include a one or two page summary of why they were asked to perform the work; a brief background on the department/agency mission being studied; the methodology used; and a summary of what they found. By their nature, GAO reports are entitled in a somewhat pessimistic manner. (i.e. Allied Forces land on Normandy Peninsula but Air Drop Accuracy was Poor"). But GAO is non-partisan and also uses the Government Audit Standards. If you just want the facts, try GAO. If you want partisan opinions, try the website for the Senate or House committee hearings, which seem to be convened to either support or embarrass an administration, depending on the majority party. ACBI members are encouraged to visit the GAO reports/testimony site as it is one of the easiest to use federal websites and

their reports are well-written and informative. Use the search box to focus on an agency, a problem area, a topic, or a time period.

Recommended Reading

ACBI members are encouraged to recommend books, articles, or studies dealing with espionage, investigations or the intelligence community that may be of interest to their fellow investigators. Learn when and why it became necessary to start investigating the backgrounds of federal employees, the motivations of some spies, and how they were uncovered. Send your recommendations to: editor@acbi.org with a brief review of why you enjoyed reading it.

Escape from Camp 14, by Blaine Harden (2012). This is a very short and quick read (about 2-4 hours) about a man who was born and spent his entire life up to age 23 in a North Korean prison camp for political prisoners. His crime? -- Being born. His father's crime? – He was related to uncles that fled to South Korea during the Korean War. His mother's crime? -- Unknown. He is doomed to a life of ignorance, malnutrition, slave labor, and forced to witness unspeakable acts of violence. Every infraction in the prison camp was punishable by death and executions were frequent. The book also helps to explain why China is in no hurry to persuade North Korea to change; and why reunification is low on South Korea's list of priorities. When the Soviet Union stopped providing fuel and fertilizer to North Korea in 1991, the country became a starving hell on earth. Now they are getting assistance indirectly from the US since thousands of trustworthy North Korean "technicians" are allowed to work in China, which exports goods for sale in the US. It is incomprehensible to Westerners why 20 million people must sacrifice their lives and their children's lives only to serve this brutal and backward communist state and leadership cult of the Kim family. One reviewer said the book made him want to declare war. Also see C-Span's interview with the author, Blaine Harden about the book. Better yet, watch the C-Span interview, then read the book.

Red Alert: How China's Growing Prosperity Threatens the American Way of Life, by Stephen Leeb (2011). This book explains how China is able to dominate manufacturing and how they use a combination of trade policy, cheap labor, government coercion, reverse engineering, bribes and industrial espionage to beat the competition. The book focuses on China's acquisition of rare earth minerals and other essential natural resources needed to produce and distribute energy (bauxite, fluorspar, indium,

manganese, tungsten, copper, gold, silver, oil, coal, etc.), especially alternative energy such as wind and solar. "All solar energy goes through China," and wind energy is not far behind, says the author. China has a long-term plan and anything that advances the country's strategic goals is tolerated if it does not harm its international standing. This is especially true for private sector innovation and entrepreneurship, which has fueled China's growth over the last 30 years. And since it's a communist country, the Chinese bureaucrats don't need to worry about getting re-elected.

Mastermind: The Many Faces of the 9/11 Architect, Khalid Shaikh Mohammed, by Richard Miniter (2011). If you had done the background investigation on KSM, as he is known in the intelligence community, you would have uncovered a wide swath of security issues. His F1 student visa was improper (His parents were too poor to own a telephone, yet KSD attended college overseas courtesy of an unknown benefactor). He targeted US schools (Chowan College, North Carolina A&T University) that welcomed students from the Middle East and did not have high admission or English language standards. He was cited for multiple moving violations, all of which he ignored. He bullied his fellow "non-Mullah" Muslim students. The author claims to be the first to thoroughly investigate KSD's background – interviewing friends, classmates, teachers, etc. It not hard to see how his personality was warped by his father's strict Salafi brand of Islam and the extraordinary events of 1979: 1) The abdication of the Shah in Iran and the rise of the Islamist theocracy; 2) the bloody attack on the Grand Mosque in Mecca; 3) the capture of the US Embassy in Iran and the murder of the US Ambassador to Afghanistan; and 4) the invasion of Afghanistan by the Soviet Army. Now was the time, he thought, to fight the decadent West and establish a new utopian version of the 7th century caliphate. Empty your jails and send your convicts to Afghanistan, to Bosnia, to Iraq, to Pakistan. The problem with KSM's vision is there is virtually no one that doesn't deserve to be punished for transgressions against his narrow interpretation of Islam. The author also highly recommends reading The Muslim Brotherhood: The Organization and Policies of a Global Islamist Movement, by Barry Rubin (2010).

The book "No Easy Day" can be purchased and read by anyone; however, the Pentagon is requesting that anyone with knowledge of the tactics or events explained in the book refrain from commenting on it verbally or in writing, as a recent article in the Virginia Pilot explains. If you want to know more about SEAL selection or basic training, and one man's death-defying mission, try reading "Lone Survivor", by Marcus Luttrell. This is definitely no country for old men.

Background Investigations in the News. Here are links to three stories that have appeared recently. The following article appeared recently on Fedsmith.com, a website that hosts articles written by a variety of authors about federal subjects. It quotes

former DOHA Judge Christopher Graham, who was a guest speaker on the second day of the March 2012 ACBI Conference.

Federal Employees Seeing Increase in Revoked Security Clearances

This next article also appeared on Fedsmith.com, and discusses an increase in the number of security clearances denied or revoked. Be forewarned as the author happens to represent employees that have their clearances denied or revoked.

Security Clearance Holder Ranks Grow; NSA & CIA Lead Denials/Revocations

In case you missed this when it was published in September 2010, and might be interested in OPM work, here is a blog entry about FY2011 changes in BI's that was posted at the always helpful website -- clearancejobs.com:

Cost of Security/Suitability Investigations -- FY 2011

Here is a helpful article about e-mail etiquette on the microsoft.com website. It lists many of the transgressions that ACBI members are known for, such as: subject does not match the content; the "me too" messages that don't add anything; answering only one of two or more questions asked; replying to all when the response is intended for one person; and failing to reply when it should be given. E-mail is a heavy consumer of work time, and CI's are not compensated for the time it takes to read them. So, let's try to be productive and courteous when using e-mail. Laura Stack, the speaker/author, is very good on the subject of productivity. See this 9 minute youtube.com clip of some of her speaking engagements, or visit her website, The Productivity Pro, if you like the e-mail tips or would like to make yourself more productive.

12 Tips for Better E-Mail Etiquette

.

Contact the Editor

Questions, comments, constructive criticism, and content recommended for publication after further research in the ACBI News is welcome. The ACBI News is published quarterly in January, April, July and October, for the benefit of the ACBI members. Write to the Editor at: editor@acbi.net with your ideas.