

Greater St. Louis Chapter News

CHAPTER 50

July 2012

From the Chapter Chair

Can you believe that summer is nearly over? Many of us have been out buying what seems like hundreds of glue sticks and boxes of crayons in an effort to locate everything on the school supply list, which gets longer every passing year.

With summer's end and back to school time for the kids comes an awesome training opportunity for security professionals in the area. Chapter 50 will be holding its first ever day-long training seminar on September 6th at the Four Points Sheraton in Fair-

view Heights, Illinois. There will be a fee to attend the event (fee TBD) and this will include breakfast and lunch. We will have presentations over FOCI, International issues, JPAS, Controlled Unclassified Information, Cyber Security, Counterintelligence, and much, much more. The chapter officers and I look forward to making this seminar a success and a worthwhile day full of learning, fun, and networking. Non-members are invited to attend and a save the date flyer and tentative agenda will be out soon.

Our chapter also just wrapped up our second meeting with a very special guest, Mr. David Berglund, Northern RDAA. There was also a recap of the NCMS seminar presented by Ms. Sherylyn Stevens of DRS. If you couldn't attend the meeting, please log into the members only section of our chapter website to access the presentations and notes.

I look forward to seeing you all in September!!!!

Thank you,

Amber Elliott, Chapter Chair

Seeking Conference Sponsors

The Greater St. Louis Chapter is seeking corporate sponsors for our Fall Conference on September 6, 2012. If you or someone you know is interested in sponsoring our seminar, please contact Amber Elliott at Elliott.Amber@bah.com. Our sponsor's logos will be featured in the next newsletter and in any material provided at the conference.



Tips For Traveling Abroad submitted by Erin Hamilton

Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. Targeting Methods include: Luggage Searches, Extensive Questioning, Unnecessary Inspection, and Downloading of information from computers. The types of critical information these cyber criminals are looking for includes: Customer Data, Employee Data, Pricing Strategies, Proprietary Formulas, Technical Components, Phone Directories, and many others. Here are some measure to ensure safety not only for you, but for your company as well when traveling abroad.

1. Don't leave any documentation or laptops at the hotel, even if it's in the safe. These safes CAN be opened by hotel security.
2. Don't discuss sensitive matters where it can be overheard (Limos, Cars, Hotels, Bars, etc.) They have well established contacts with hotels, taxis, and airlines.
3. Be suspicious of quick friendships
4. Don't use black market currency exchanges (street kiosks).
5. Perform risk assessment for the specific place you are going (www.osac.gov)
6. Don't bring any unnecessary items (wallets, purses, etc) if not needed.
7. Replace your memory card on your camera before you leave.
8. Don't attempt to locate surveillance equipment in hotel rooms (gives more credence to search your items)
9. Be suspicious if singled out in a group. They tend to separate the weakest link.
10. Take inventory of your luggage items if it goes missing.
11. Don't wear company logo on your clothing.
12. Keep a low profile and shun publicity.
13. Do not use non-company computers to log in to company's network.

September

6

Save the Date.....

Please mark your calendars for our first chapter seminar. The seminar will be held on September 6th at the Four Points Sheraton in Fairview Heights, IL. We have a great day of training lined up including cyber security, counterintelligence, controlled unclassified information, FOCI, and international (just to name a few). The full agenda will be out in a couple of weeks along with the RSVP information. Non-NCMS members are welcome, so please tell your friends!!

DSS News

submitted by Erin Hamilton



Periodic Reinvestigations – Effective 1 August 2012, the Defense Industrial Security Clearance Office (DISCO) will only accept requests for periodic reinvestigations that are within 90 days of the investigation anniversary date. This is a change from the previous six-month (180 days) timeframe. The reduced time frame is consistent with improved Industry security clearance investigation/ adjudication times. Periodic Reinvestigation requests already initiated at DISCO will continue to be processed as appropriate.

http://www.dss.mil/disco/indus_disco_updates.html

DoD Services Call Center – Email Encryption - The DoD Security Services (Call) Center (888-282-7682) has implemented digital encryption capability for use with its two customer service e-mail contact accounts/addresses (Account.Request@DSSHelp.org and Call.Center@DSSHelp.org). Please see below link for instructional guide.

<http://www.dss.mil/documents/Group-Mailbox-PKI-Use.pdf>

Security Clearance Request Rejections – The most common causes of rejection include submission of application packages with incomplete information, e.g., subject not including the company submitting the investigation request as a current employer, missing SSN for spouse or co-habitant, fingerprint cards, information for relatives and failing to provide Selective Service registration information or legal exemption.

The following issues account for 96% of investigation requests being rejected by DISCO:

1. Missing employment information
2. Missing Social Security Number of Spouse or Co-Habitant
3. Missing Relatives Information
4. Missing Selective Service Registration Information

5. Incomplete information concerning debts or bankruptcy
6. Missing Education Reference Information
7. Missing Employment Reference Information
8. Incomplete Explanation of Employment Record
9. Missing Personal Reference Information
10. Missing Explanation of Drug Usage

The following issues account for 96% of investigation requests being rejected by OPM:

1. Fingerprint cards not submitted within timeframe
2. Certification/Release Forms Illegible
3. Certification/Release Forms Not Meeting Date Requirements
4. Discrepancy in Place and Date of Birth Information
5. Missing References
6. Discrepancy of e-QIP Request #
7. Missing Employment Information
8. Certification / Release Forms Not Submitted
9. Missing Education Information
10. Missing Residence Information

<http://www.dss.mil/documents/disco/Common-Reasons-Clearance-Request-Is-Unacceptable.pdf>

CDSE Upcoming Webinars –

Security Rating Matrix: Tuesday, August 7, 2012
(10:30 CDT and 1:30 CDT)

Activity Security Manager Responsibilities: Wednesday, August 22, 2012 (1:30 CDT)

<http://www.dss.mil/cdse/catalog/webinars/index.html>



EEOC ISSUES GUIDANCE ON CRIMINAL BACKGROUND CHECKS, BUT RETAINS EMPLOYER PROTECTIONS FOR POSITIONS OF NATIONAL SECURITY

By: Brian E. Kaveney, Zachary C. Howenstine, Lindsey R. Selinger

The Equal Employment Opportunity Commission (EEOC) recently issued its highly anticipated Enforcement Guidance regarding employer use of arrest and conviction records and compliance with Title VII of the Civil Rights Act of 1964. The EEOC has long expressed its commitment to the issue, as evident in its 1987 and 1990 releases, as well as the meeting it held to discuss the issue on July 26, 2011. The Guidance results from the EEOC's findings that criminal record exclusions generally cause a disparate impact and may be founded on incomplete and inaccurate information. To address the problems it identified, the EEOC issued the Guidance and a corresponding "Best Practices" list for employers to consider to ensure compliance with Title VII.

Guidance

The EEOC advises employers to reconsider their present applications and remove blanket, "catch-all" questions that ask whether the individual has been convicted of any crimes. If and when an employer chooses to make inquiries on this topic, the employer should be able to demonstrate that the criminal background information is job-related and consistent with business necessity.

The Guidance also makes clear that the EEOC believes the use of *arrest* records in employment decisions is neither job related nor consistent with business necessity, and therefore, does not comply with Title VII. In fact, the use of arrest records has long been discouraged by the EEOC because an arrest, unlike a conviction, does not establish that criminal conduct has occurred, nor does it report the final outcome of the arrest. Accordingly, an employer's decision to exclude an applicant on the basis of an arrest alone would be considered a violation of Title VII. However, consistent with the overarching theme of the Guidance, an employer may consider the underlying conduct referenced in the arrest report if the conduct makes the individual unfit for the position at issue.

Somewhat similar to the mitigating conditions available in the *Adjudicative Guidelines for Determining Eligibility for Access to Information*, the Guidance

counsels employers to consider the following factors when analyzing an applicant's criminal history:

- (1) the nature and gravity of the offense or offenses (which the EEOC explains may involve evaluating the harm caused, the legal elements of the crime, and the classification, i.e., misdemeanor or felony);
- (2) the time that has passed since the conviction and/or completion of the sentence (which the EEOC explains as looking at particular facts and circumstances and evaluating studies of recidivism); and
- (3) the nature of the job held or sought (which the EEOC explains requires more than examining just the job title, but also specific duties, essential functions, and environment).

As in the whole person concept in clearance decisions, the EEOC indicates its preference for employer use of individualized assessments when making employment decisions based on criminal background information, and these assessments can be offered by the employer in response to a challenge from the EEOC or an individual litigant. This assessment includes:

- The facts or circumstances surrounding the offense or conduct;
 - The number of offenses for which the individual was convicted;
 - Older age at the time of conviction, or release from prison;
 - Evidence that the individual performed the same type of work, post conviction, with the same or a different employer, with no known incidents of criminal conduct;
 - The length and consistency of employment history before and after the offense or conduct;
 - Rehabilitation efforts, e.g., education/training;
 - Employment or character references and any other information regarding fitness for the particular position; and
- Whether the individual is bonded under a federal, state, or local bonding program.

Continued next page

EEOC ISSUES GUIDANCE ON CRIMINAL BACKGROUND CHECKS Continued

Criminal Background and Security Clearance

The EEOC acknowledges that some industries are subject to federal statutory and/or regulatory requirements that prohibit individuals with certain criminal records from obtaining or holding particular positions. By way of example, the EEOC notes that “federal law excludes an individual who was convicted in the previous ten years of specified crimes from working as a security screener or otherwise having unescorted access to secure areas of an airport.”

Similarly, Title VII includes a national security exception that permits an employer to decline to employ an individual because he or she cannot satisfy the federal security clearance requirements. In other words, if a security clearance is required for the applicant’s position, an employer may in *some* circumstances deny employment based on the applicant’s failure to obtain a security clearance if the following requirements are met:

- First, the position must be subject to national security requirements imposed by federal statute or Executive Order.
- Second, the adverse employment action must result from the denial or revocation of a security clearance.

Thus, the exception only permits an employer to revoke an offer of employment or terminate an employee after the government has issued an unfavorable security clearance determination. It seemingly does not apply to situations where an employer chooses not to hire an applicant because the applicant discloses a criminal record that would make it difficult for the applicant to obtain a security clearance.

Questions therefore remain about whether an employer hiring for national security positions may continue to utilize a blanket criminal background question on its applications. The answer appears to be yes, but with caution. The overarching point of the EEOC’s Guidance is that an employer may lawfully consider an applicant’s criminal record in making an employment decision, provided the criminal record is relevant to the job position and denying employment on that basis is consistent with a legitimate business necessity. For positions that require a security clearance, the extent and nature of an applicant’s criminal history is, of course, highly relevant to whether the applicant will be able to obtain a clearance (and therefore satisfy the minimum job requirements). Significantly, EEOC Commissioner Victoria Lipnic observed in the Guidance that “[there may be times] when particular criminal history will be so manifestly relevant to the position in question that an employer can lawfully screen out an applicant without further inquiry.” Furthermore, in arguably borderline cases—for example, where the applicant discloses an isolated yet serious criminal offense that occurred decades ago—the employer may be able to point to the potential time and cost associated with adjudicating a security clearance application as a business necessity that warrants excluding the applicant from employment. Most importantly, the employer should be sure to incorporate into all employment decisions (1) consideration of the three factors identified by the EEOC in the Guidance and discussed above; (2) an individualized assessment of the applicant; and (3) implementation of “Best Practices” patterned on the list provided by the EEOC.

Continued next page

First ISP Certification Earned for Chapter 50

Congratulations to Lynette Whitehead of ESRI for earning her ISP certification at the 2012 National Seminar in Orlando!!!



EEOC ISSUES GUIDANCE ON CRIMINAL BACKGROUND CHECKS Continued

Best Practices

In an effort to provide practical implementation guidance, the EEOC also provides a “Best Practices” list for employers’ consideration:

- Eliminate policies or practices that exclude people from employment based on any criminal record;
- Train managers, hiring officials, and decision-makers about Title VII and its prohibition on employment discrimination;
- Develop a narrowly-tailored written policy and procedures for screening for criminal records;
- Identify essential job requirements and the actual circumstances under which the jobs are performed;
- Determine the specific offenses that may demonstrate unfitness for performing certain jobs;
- Identify the criminal offenses based on all available evidence;
- Determine the duration of exclusions for criminal conduct based on all available evidence;
- Record the justification for the screening policy and procedures;
- Note and keep a record of consultations and research considered in crafting the policy and procedures;
- Train managers, hiring officials, and decision-makers on how to implement the policy and procedures consistent with Title VII;
- When asking questions about criminal records, limit inquiries to records of those specific offenses the employer has identified as demonstrating unfitness for performing certain jobs, so that it is clear that any exclusion on that basis was job-related and/or consistent with business necessity; and
- Keep information about the criminal records of applicants and employees confidential (that is, only use it for the purposes for which it was collected).

The EEOC’s Guidance strongly suggests that employers adhering to these guidelines will be in a position to provide an effective rebuttal to any subsequent challenges to employment decisions from the EEOC or individual applicants. Accordingly, facility security officers should share this article with human-resource personnel.

If you have any questions, please do not hesitate to contact Brian Kaveney at bkaveney@armstrongteasdale.com



Spotlight Security Professional

In our next edition, we will add a spot light security professional section!!! To volunteer or nominate one of your peers, please email Amber Elliott, or visit our chapter website: <http://www.ncms-stlouis.org>, and select “Spotlight FSO” in the left column followed by the nominate selection.



Safeguarding Responsibilities

submitted by Erin Hamilton

Safeguarding classified material is the upmost important responsibility. It's our job to keep our team's refreshed on their safeguarding responsibilities. Below are some safeguarding tips that can be used for keeping everyone aware.

1. Only designated GSA-approved containers may be used for storing classified material. When classified material is removed from its container, it must remain under the direct supervision of an authorized appropriately clearance employee at ALL times.
2. Employees should choose private office space or other approved areas to perform classified work. Should an unauthorized person enter your work area while classified work is in progress, the classified material should be covered or turned over. Never place classified material inside a desk or other unapproved container for any length of time.
3. Do not provide classified information to another individual unless that person has the proper level security clearance, and the need-to-know for the information involved. Physically check the person's identity by personally reviewing an official form of photo identification such as a driver's license, passport, or credentials. Compare the photo against the individual's appearance. Compare identifying information against employee records or against a visit authorization letter on file in the security office.
4. Do not attempt to "talk around" classified information over the telephone, unless you are using an authorized secure telephone line.
5. Do not remove classified material from this facility without prior approval from the Facility Security Officer or his/her designee.
6. Do not enter classified information into any automated information system, to include computers, test equipment, etc., without the prior approval of the Facility Security Officer.

Mentoring Program

Each chapter is required to have a mentoring program on a local level that falls under the national program. There are three levels of mentoring to include initial, intermediate, and advanced. To learn more about the mentoring program, visit the members only section of the national website. If you are interested in becoming the Mentor Program Committee Chair, please contact Amber Elliott, Chapter Chair.

In the News—Canadian Spy Sells American Secrets

A Canadian naval officer arrested this year for allegedly leaking secrets may also have compromised top level Australian, British and American intelligence, a report said Wednesday. Jeffrey Delisle, a naval intelligence officer, was charged in Canada in January with communicating over the past five years "with a foreign entity, information that the government of Canada is taking measures to safeguard".

Canadian reports said Ottawa expelled four Russian diplomats in the aftermath of Delisle's arrest, although Moscow denied this. On Wednesday the Sydney Morning Herald, citing Australian security sources, said Delisle also allegedly sold to Moscow signals intelligence—information gathered by the interception of radio and radar signals -- collected by the United States, Britain, Australia and New Zealand.

It said much of the information was more highly classified than the disclosures attributed to US Private Bradley Manning, who is accused of

releasing a vast cache of classified files to whistle blowing website WikiLeaks. The newspaper said Delisle was the subject of high-level consultations between the Australian and Canadian governments and was discussed at a secret international conference in New Zealand earlier this year.

An Australian security source quoted by the newspaper said Delisle's access was "apparently very wide" and that "Australian reporting was inevitably compromised". "The signals intelligence community is very close, we share our intelligence overwhelmingly with the US, UK and Canada," a former Australian Defense Signals Directorate officer said.

An Australian Defense Department spokeswoman said the government did not comment on

intelligence matters. "However, the Australian government takes national security very seriously and is continually reviewing and

strengthening policies, practices and techniques to ensure Australia's national security," she told AFP.

New Zealand Prime Minister John Key refused to confirm whether the intelligence conference took place and said he could not discuss matters of national security. "I'm not in a position to be able to, or want to, comment on our national security," he told reporters. "These things are sometimes better left unsaid." Delisle's offences allegedly occurred in the Canadian capital Ottawa, Halifax and in towns in Ontario and Nova Scotia provinces, court documents said. He has been charged under Canada's Security of Information Act, with a conviction carrying a maximum penalty of life in prison. (Yahoo News)

<http://news.yahoo.com/canada-spy-sold-us-australia-uk-secrets->

Holiday Cards for the Troops submitted by Sherylyn Stevens

Calling all STAMPERS!! Volunteers are needed for rubber stamping holiday cards that will be shipped to our deployed Heroes!! These handmade cards will be shipped to our Heroes in harm's way, who can add their own sentiments to send to their love ones.

We can't accomplish this awesome goal without YOU! This is a team effort. Together; we can make a real difference to our troops who are missing home during the holidays!

Thank you for your support of our heroes!

When: Sunday, August 26

Time: 12:00 to 6:00 PM

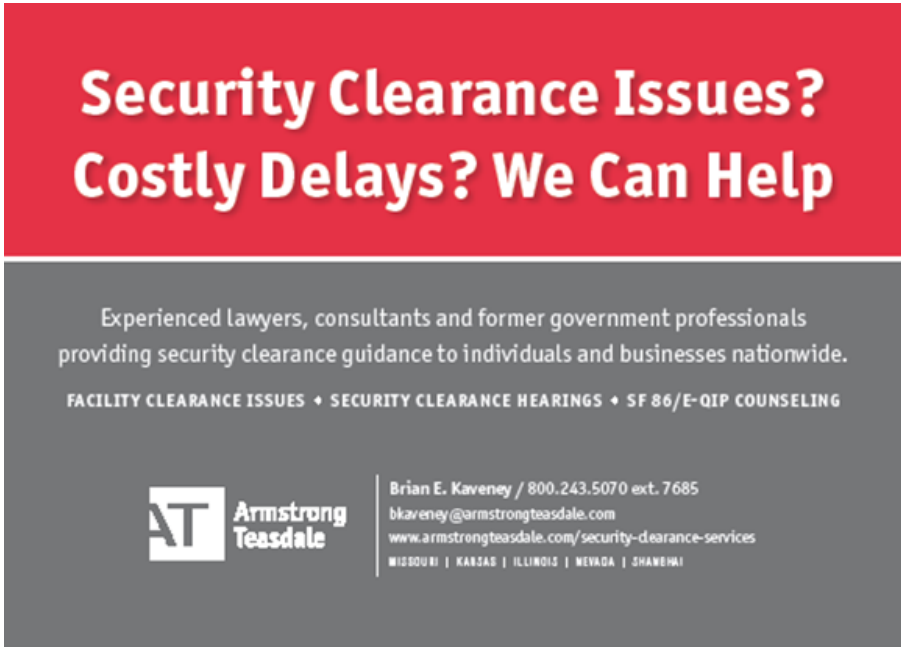
Where: Drury Inn & Suites Hotel (Ballroom) O'Fallon, IL Enter at main lobby and watch for signs

Details: All supplies for the cards will be provided. No stamping experience necessary. Helpers will be available. NO ADMISSION

Contact: Bev Penick at bjpenick@charter.net




Thank You to our Sponsors...




**Security Clearance Issues?
Costly Delays? We Can Help**

Experienced lawyers, consultants and former government professionals providing security clearance guidance to individuals and businesses nationwide.

FACILITY CLEARANCE ISSUES • SECURITY CLEARANCE HEARINGS • SF 86/E-QIP COUNSELING

 **Armstrong Teasdale**

Brian E. Kaveney / 800.243.5070 ext. 7685
bkaveney@armstrongteasdale.com
www.armstrongteasdale.com/security-clearance-services
MISSOURI | KANSAS | ILLINOIS | NEVADA | SHANGHAI



Your company could be listed here!! Contact Amber Elliott for more information on how to sponsor our chapter.



GENERAL DYNAMICS

Ordnance and Tactical Systems



Check Out Our Website

Please contact Dennis Beasley to add/remove content from our chapter website.

Dennis.Beasley@njvc.com

<http://www.ncms-stlouis.org>



Greater St. Louis Chapter Officers			
Chair	Amber Elliott	BAH	Elliott_Amber@bah.com
Vice Chair	Erin Hamilton	SRA	Erin_Hamilton@sra.com
Secretary	Beverly Penick	MITRE	penick@mitre.org
Treasurer	Don Wright	SAIC	Donald.w.wright@saic.com
Greater St. Louis Chapter Committees			
FOCI	Gary Bledsoe	GKN	Gary.Bledsoe@usa.gknaerospace.com
Meetings Committee	Amber Elliott (Chair)	BAH	Elliott_Amber@bah.com
	Terri Moran	DRS	TMoran@drs-ssi.com
	Sue Falk	DRS	SFalk@drs-ssi.com
	Edd Pope	TASC	Edward.Pope@tasc.com
Training Committee	Chapter Officers		
Membership Committee	Jo Ann Covington	NJVC	JoAnn.Covington@njvc.com
	Ruth Hoffecker	GD-OTS	Ruth.Hoffecker@gd-ots.com
	Justin Rix	GD-OTS	Justin.Rix@gd-ots.com
ISSC Co-Chairs	Sherylyn Stevens	DRS	SStevens@drs.com
	Dennis Beasley	NJVC	Dennis.Beasley@njvc.com
Website Committee	Dennis Beasley	NJVC	Dennis.Beasley@njvc.com

If you are interested in joining a committee, please contact Amber Elliott, Chapter Chair

Welcome New Members



Bruce Vincent	DRS
Deborah Wiedner	Global Velocity
Linda Lezner	Unitech Consulting
Michele Diehl	Stauder Technologies
Robert Cundall	DRS
Michael Pratcher	DISA
Chuck Peterson	BAE
Kevin Cox	Armstrong Teasdale

It is never too early to start planning for next year!!

The 49th Annual Seminar, Security...Strong as the Chicago Wind, will be held in Chicago, IL at the Palmer House Hilton.



AskDISCO Webinar submitted by Janet Reese

On July 24, 2012, DISCO launched its first "AskDISCO" webinar. And while there were multiple technical difficulties, most of those attending appeared to think the "AskDISCO" webinar was well worth continuing the sessions.

This first webinar dealt with the eligibility policy change taking the eligibility window for periodic reinvestigations (PRs) down from 180 days to 90 days. The webinar covered the basics such as the following:

- Those with access to Top Secret and Secret levels be reinvestigated at 5-year and 10-year intervals accordingly
- Anniversary dates are from the closing date of the previous investigation.
- e-QIPs for an employee's PR must be submitted no later than the due date
- To ensure DISCO and OPM can meet the suspense, e-QIPs for PR may be initiated up to 3 months in advance of due date
- DISCO will reject e-QIP submissions outside of 90 days starting August 1, 2012
- Monthly reports of overdue PRs and request e-QIPs for PRs will be run by DISCO
- If e-QIP for a PR is not submitted within 30 days of the overdue notification, the eligibility (without prejudice) from JPAS will be withdrawn
 - DISCO will issue a No Determination Made (NDM)
 - Only when the e-QIP is received by DISCO, then will the previously valid eligibility will be reinstated

- Applicants may request information by sending a letter to DMC under the Privacy Act.
DMC, Privacy Act Office
PO Box 168
Boyers, PA 16020-0168
- Recommendation:
 - Check your JPAS account frequently
 - If sole FSO and if JPAS account manager, recommend you request Level 7 access as well as Level 4
 - Send SAR to DMDC to request Level 7 access

The webinar also covered Reciprocity, RRU's, and the OCONUS Project.

- Reciprocity: eligibility for investigations that have been favorably adjudicated by another agency
- RRU's: are only for specific requests, which are posted on the DSS website (http://www.dss.mil/disco/indus_discomaintain.html#research)
- OCONUS Project: a joint effort between OPM, DSS, and Industry partners to have OPM establish a presence in Kuwait

There were a great many questions fielded by the DISCO hosts; however, because of the technical difficulties it was hard to hear the answers. In response, DISCO had said they would post the webinar on the site.