



KCJIS NEWS

MAY 2016

SECURE MAIL FROM THE KBI WILSON WILEY, IT SECURITY ANALYST II KBI

In the very near future, you may receive a couple emails from the KBI that look a little different. Different how? They will have a big KBI logo and banner across the top, they will say "KBI Secure Mail Message," and they will have a link to click or a password. What is this? The KBI recently implemented a new secure mail messaging solution to be able to securely send and receive sensitive information from our law enforcement and criminal justice partners. Why did we do this? Not all emails are created equal. Some emails are not encrypted when they're transferred from one email server to another. We couldn't guarantee that emails with sensitive information would be transferred securely. With the secure mail solution, the entire communication between our server and your computer is encrypted, and the data on our server is encrypted while it waits for you to download it.

Disclaimer: Please keep in mind that dissemination and transfer of sensitive information, albeit encrypted, is still subject to all applicable laws, rules, regulations, policies and procedures of KCJIS, CJIS, Federal, Kansas, county, city, agency, department, etc.

INSIDE THIS ISSUE

SECURE MAIL	1-2
END OF QUICK-TIME	2
PATC TRAINING	3
RANSOMWARE	3
NIBRS REPORTING	4
KBI TRAINING	4
ALIAS NAMES	5
NICS REQUESTS	5
KCJIS & CLOUD COMPUTING	6
KBI HELP DESK	7
OFFENDER REGISTRATION	8
INVOLUNTARY COMMITMENTS	8-9
KCJIS CONFERENCE	9

Now that that's out of the way, how does this work? When someone at the KBI sends you a secure mail message, you will receive two emails. The first email will contain a link to click:



Kansas Bureau of Investigation

Derek Schmidt, Attorney General
Kirk Thompson, Director

KBI Secure Mail Message

The following file(s) have been sent to you from @KBI.STATE.KS.US. To download, please click on the following link.

[Click here to download the file\(s\) listed below](#)

Sensitive Spreadsheet.xlsx 8.54 KB

If the link above does not open, please copy and paste the following URL into your browser:

<https://securemail.kbi.ks.gov>

The second email will contain an accompanying unique password to view the secure mail message:



Kansas Bureau of Investigation

Derek Schmidt, Attorney General
Kirk Thompson, Director

KBI Secure Mail Message Password

The password for a secure message has been sent to you from @KBI.STATE.KS.US. Please enter this password when accessing your message.

Password:

SECURE MAIL FROM THE KBI, CONTINUED WILSON WILEY, IT SECURITY ANALYST II KBI

When you click the link in the first email, your web browser will come up and load the website to the right. At the password prompt, you will enter the password you received in the second email into the password field and click the 'Submit' button. Your secure mail message will then be loaded.



Secure Mail [Reply to Sender](#)

From: @KBI.STATE.KS.US
 Sent On: 4/13/16 5:02:56 PM
 Subject: Sensitive Information
 Message: Here is the sensitive information.

Attachments (click on the file name to download)

File	Size	Remaining
Sensitive Spreadsheet.xlsx	8.54 KB	1

You will see the contents of the secure mail message that was sent to you, as well as the attachments, which you can click to download. The page will tell you how many more times the attachment can be downloaded. **Each attached file can only be downloaded one time, so be very careful when you click the attachment link that you save the file completely and in a secure location on a secure computer that you will be able to locate later.**

If you have information to send back to the person at the KBI, you can click the 'Reply to Sender' button. This will take you to a page where you can compose your reply message and attach your own files to send back securely. When it's ready, just click the 'Send' button and the person at the KBI will get a notification that you have sent them a secure mail message. Your reply message and data will be transferred to the KBI and stored encrypted.

You won't be able to initiate a secure mail conversation with someone at the KBI. Someone at the KBI will have to initiate the secure mail conversation and you will be able to reply to their message.



Reply to Sender [Send](#) [Cancel](#)

To: @KBI.STATE.KS.US
 Subject: RE: Sensitive Information

Message

From: @KBI.STATE.KS.US
 Sent: 4/13/16 5:02:56 PM
 To: Wilson.Wiley@KBI.STATE.KS.US
 Subject: Sensitive Information
 Here is the sensitive information.

Attachments
[Click here to attach a file](#)

THE END OF QUICKTIME FOR WINDOWS ROD STROLE, PROGRAM CONSULTANT II KHP

Apple no longer provides security updates for QuickTime. Therefore, QuickTime could become vulnerable to attacks. An identified vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of QuickTime. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

Computer systems running unsupported software are exposed to elevated cybersecurity dangers, such as increased risks of malicious attacks or electronic data loss. Exploitation of QuickTime for Windows vulnerabilities could allow remote attackers to take control of affected systems.¹

Per KCJIS Policy 5.10.4.1, *Patch Management* "...if a vendor has announced they will cease support, especially the patching of a product, after a specific date, that particular product will no longer be considered compliant with the Patch Management policy requirement once that vendor announced date is reached." Therefore, as a precaution (and also a recommendation from Apple), QuickTime should be uninstalled or removed from systems that have access to KCJIS.

¹US-CERT, Alert TA16-105A "Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced" 14 APR. 2016 <<https://www.us-cert.gov/ncas/alerts/TA16-105A>>.

PRACTICAL KINESIC INTERVIEW AND INTERROGATION TRAINING DONNA BEVITT, TRAINING COORDINATOR KBI



The Kansas Bureau of Investigation is excited to announce that we will be hosting Practical Kinesic Interview and Interrogation week-long training August 8th through August 12th, 2016. Training will be provided by Stan B. Walters, "The Lie Guy". This training opportunity will include both basic and advanced level courses. Stan Walters with the Public Agency Training Council will be on site to provide the training courses and pass on the skills needed for today's law enforcement professional investigator. This is a great opportunity to gain, or take a refresher course, in interview and interrogation skills. Seating will be limited so please register soon. Register to attend the Kansas Practical Kinesic Interview and Interrogation training on the following link: <http://www.patc.com/training/schedule.php>.

The training will be delivered at the new KBI Forensic Science Center 2001 SW Washburn Ave. Topeka, KS 66604. This will be a great opportunity to see and experience our new forensic center, spend time with fellow law enforcement staff and attend some really great training. Course fees will be \$495.00 per person which will include the full 40 hours of training credit hours. Hotel accommodations are offered by Capitol Plaza Hotel for \$72.00 a night and reservations can be at 785-431-7200. Capitol Plaza Hotel is located at 1717 SW. Topeka Blvd. Payment information can also be found on the website and payments should be submitted to the Public Agency Training Council. We are pleased to have the opportunity to host this training event and are proud to extend an invitation to our local law enforcement partners.

Training Event Distribution List

If you or other law enforcement personnel from your agency would like to be included to the KBI law enforcement training distribution listing please contact Donna Bevitt at donna.bevitt@kbi.state.ks.us or 785-296-8289. I will ensure that you are added to the list to receive training event announcements and information from our agency and other law enforcement agencies.

RANSOMWARE IS STILL MAJOR CYBERSECURITY THREAT FOR 2016 TAMMIE HENDRIX, IT SECURITY AUDITOR/TRAINER KHP

Ransomware has become a big topic this year and its impact is growing. It can be performed on all device platforms including Windows, Android and Apple/Mac. Ransomware is a type of malware that holds your mobile device or computer hostage and prevents users from accessing their computer. It forces its victims to pay the ransom through certain online payment methods. You can expect to see much more of it because paying the ransom is the easiest way for many businesses and individuals to get their data back.

The best defense that will defeat ransomware is to eliminate the need to pay a ransom. Do this by performing regularly scheduled backups. Backups should use a second path and login credentials other than what you normally use. For example, backup to an external media device such as tape or optical disk drive. Another option is to use a special login used just for back up and restoration when backing up to a different location on the network that your standard "user" login cannot access.

Make sure your anti-virus software is using a current malware (signature) list to compare against, and that it is always running. Enable any "real time" or "heuristic" scan features in order to recognize new threats faster based on behavior of programs running on your device(s). Refer to KCJIS policy and procedure 5.10.4.2 regarding Malicious Code Protection. Also, policy 5.10.1.3 requires network-based and/or host-based intrusion detection be installed. Seal as many holes and cracks in your systems defenses as possible by patching and updating all software...including the operating system, the browser and all the plug-ins that the browser typically uses, and other applications – particularly commercially available programs like your office suite, pdf maker, and media players.

Make sure everyone is completing security awareness training and that they understand rules and best practices regarding unexpected emails, their attachments, and links to potential dangerous web sites. A little forethought, better education and keeping software up to date helps minimize the likelihood that your system has an exposed vulnerability on it.

FBI ANNOUNCES PUSH TO END SUMMARY DATA (SRS) AND TRANSITION TO 100% NIBRS REPORTING

MITCH BEEMER, INCIDENT BASED REPORTING UNIT MANAGER KBI

The FBI Director has made the transition from the Summary Reporting System (SRS) to the National Incident-Based Reporting System (NIBRS) a top priority. This transition is also supported by the International Association of Chiefs of Police, Major Cities Chiefs Association, Major County Sheriffs' Association, and the National Sheriffs' Association, as well as the Executive Branch of our government. On February 9, 2016, the FBI Director signed the Advisory Policy Board recommendation:

"The FBI UCR Program will transition to a NIBRS-only data collection by January 1, 2021, and will evaluate the probability of achieving that goal on an annual basis. Federal, state, local, and tribal agencies unable to meet the five year transition and who have committed to transitioning to NIBRS will collaborate with the FBI CJIS to develop a transition plan and timeline for conversion."

For many states this announcement signaled the need for major changes and/or improvements in their crime reporting abilities. However, for the majority of Kansas Law Enforcement agencies the transition to NIBRS was completed years ago. Most Kansas law enforcement agencies have been submitting their incident based reports, and data, to the Kansas Incident Based Reporting System (KIBRS) for years. There are still a few agencies who submit their Summary Data (SRS) to the KIBRS unit for submission to the FBI, but several of these agencies are already in the process of exploring ways to be able to submit NIBRS data to the Kansas Bureau of Investigation. It is the goal of the Kansas Bureau of Investigation to have all Kansas LEA submitting NIBRS data well in advance of the 2021 deadline.

When used to its full potential, the UCR Program's National Incident Based Reporting System (NIBRS) identifies with precision when and where crime takes place, what form it takes, and the characteristics of its victims and perpetrators. Armed with such information, law enforcement can better define the resources it needs to fight crime, as well as use those resources in the most efficient and effective manner.

If your agency has any questions about NIBRS reporting, please contact the Incident Based Reporting unit at the KBI:

Mitch Beemer
Incident Based Reporting Unit Manager
(Office) 785-296-8279
(Fax) 785-296-6781
Mitch.Beemer@KBI.STATE.KS.US

Connie Molina
Program Consultant I
Incident Based Reporting
(Office) 785-296-8278
KIBRS Duty Line- 785-296-4373
(Fax) 785-296-6781
Connie.Molina@KBI.STATE.KS.US

UPCOMING KBI TRAININGS

CONNIE MOLINA, PROGRAM CONSULTANT I KBI

The Kansas Bureau of Investigation will be offering training opportunities in the following locations in July and August 2016. For more information on the training schedule and registration, please go to the calendar on the KCJIS web portal at <https://kcjis.ks.gov>.

Register early as seating is limited!

- Barton County—Tuesday, July 12th
- Valley Center—Wednesday, July 13th
- Oswego—Thursday, July 14th
- Emporia/Lyon Co—Tuesday, August 2nd
- Junction City—Tuesday, August 23rd

Sessions Offered:

- 10 Print Fingerprint Identification
- Criminal History Records
- Rapsheet Differences
- Kansas Incident Based Reporting System (KIBRS)
- Offender Registration

USING AN ALIAS IN DOCUMENTATION VANESSA RINE, PROGRAM CONSULTANT I KBI

The KBI has noticed an increase in questions regarding alias names and the general process for changing reported information. In order to ensure that both the KBI and FBI have the correct information, please refer to the following process:

Criminal Records: When an individual is booked or housed at a jail, it may be discovered that the individual is using another identity or has used another identity in the past. When fingerprinting an individual, you must fingerprint them with the identity they gave at the time of arrest. It is possible through prior contact with the individual that you know them by a different identity. Please put all the other identities, including the true identities, in the alias portion of the fingerprint card for that arrest. This will insure all known names will appear on the 'rapsheet'.

Kansas Incident Based Reporting: The Booking information, Kansas Arrest Reports (KSARs), and Kansas Offense Reports (KSORs) will have already been generated with the identity the individual claimed upon arrest. The name will need to be updated to the individual's correct name on the Offense and Arrest Reports, but not on the fingerprint card. For KSORs, please resubmit the report with the corrected name and the *modify* box checked. For KSARs, please submit a deletion request and submit a new KSAR with the correct name.

*Please note that Change Request forms should ONLY be used by the arresting agency to update a previously submitted arrest. Please also note that you CAN NOT change the fingerprint card via livescan and resend it electronically without also sending in a Change Request form to the KBI Criminal History Records Unit. Doing so will update the Kansas side of the record, but it will not update the federal record as this is a manual process for the KBI. The FBI will not change their master name. The only option is to add the true information to the federal record as an AKA.

RESPONDING WITHIN 72 HOURS TO NICS REQUESTS GINNY EARDLEY, NICS COORDINATOR KBI

The National Instant Criminal Background Check System (NICS) is a record check database that works to enforce the Brady Handgun Violence Prevention Act of 1993. The FBI and KBI work together to help update Kansas Criminal Records in this database in order to prevent firearms from being sold to ineligible individuals. A list of disqualifiers for owning a firearm is listed on the FBI website at <https://www.fbi.gov/nics> under Fact Sheet. The FBI has the final say in NICS determinations.

Often the FBI, the KBI or other state Points of Contact for NICS will contact law enforcement agencies to gather additional information about a person's criminal record in order to accurately update information.

It is important that arresting agencies, prosecutors and courts work with the FBI, the KBI, and other states to obtain the most complete and accurate documentation for NICS firearms determinations. When a request from the FBI, KBI, or another state comes to one of the agencies in our state, response time for this request should be within 72 hours. Once the 72 hour timeframe has passed, the individual may be authorized to proceed with the purchase without the updated criminal history information. The fastest way to get requested criminal history information to the FBI, the KBI, or other states who have requested information for NICS purposes is to send a Fax.

When responding to NICS requests please send entire arrest reports, complaints, journal entries, and diversion agreements. Information needed for a NICS determination includes the relationship of the offender to the victim, the severity level of the convicted crime, and sentencing timeframes.

For inquiries on charges reported as a Warrant or as Failure to Appear a copy of the original journal entry is necessary. If the case was outside of your jurisdiction, please indicate where it was transferred.

It is possible for your agency to receive a request for the same record from the FBI, KBI, and another state on the same individual and/or same case. When this happens, please send the disposition and the additional record checks to the KBI to have the record updated. Once the record is update KBI can contact the FBI and/or the other state with the disposition information.

The Kansas NICS Coordinator is Ginny Eardley. You can reach her at 785-296-8244. The KBI NICS fax number is 785-368-6376.

KCJIS & CLOUD COMPUTING

KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT



The Kansas Highway Patrol (KHP) Criminal Justice Information Services (CJIS) Technical Security Team periodically fields questions from agencies regarding cloud computing as it relates to compliance with KCJIS Security Policy. The questions that are often asked are, “Can an Agency be compliant with the KCJIS Security Policy and also cloud compute?” or “Can we email Criminal Justice Information (CJI) or store CJI files in the cloud?”

Because the KCJIS Security Policy is device and architecture independent (Section 2.2), the answers to the questions above are: “it depends”. That is NOT very useful! But in reality it is factual that cloud computing can be accomplished – **provided that the vendor of the cloud technology is able to meet the existing requirements of the Security Policy**. The security policy must be reviewed in its entirety as it relates to the security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

KCJIS Policy Section 5.10.1.5 begins to address ‘Cloud Computing’. It is more of a discussion with only 2 Cloud Computing specific policies at the end.

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, National Institute of Standards and Technology (NIST) Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider’s policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

*The **metadata derived from CJI shall not be used by any cloud service provider** for any purposes.*

*The **cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.***

Appendix G.3 beginning on page 136 of the KCJIS Policies and Procedures manual, is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance. As the FBI points out in Appendix G.3, many criminal justice agencies are looking for ways to attain greater efficiency, while grappling with reduced budgets. The idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with CJI, security and policy compliance concerns are bound to arise.

For those agencies considering Cloud Computing and wanting to achieve KCJIS Security Policy compliance, it would be good to not only review Appendix G.3, but also refer to the other materials referenced in the policy area. Many of those resources are available from the FBI.gov CJIS security resource center: <https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>.



NEWS FROM THE KBI HELP DESK

JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN III KBI

Entering Stolen Decal Sticker

A correction to the last KCJIS Newsletter is needed concerning stolen decal stickers. The incorrect article explained how to enter a stolen decal sticker into the National Crime Information Center (NCIC). The Kansas Department of Revenue (KDOR) reissues the same decal number to replace the stolen decal. Because of this the KCJIS Unit has determined Kansas would no longer enter Kansas decals into NCIC. However, if a decal is stolen from an out of state tag within Kansas jurisdiction, then it is permissible to enter the decal into NCIC as follows. Use the Enter Article - EA message key. Use the Code 'JSTICKE' in the Type field, 'DECAL' in the Brand field and the decal number in the SER field. Finally, indicate that this is a stolen decal sticker from a vehicle plate in the Miscellaneous Information field. It is important to understand only out of state issued decal stickers are allowed entry into NCIC.

New Interpol Stolen Gun Query

Interpol has stood up two new message keys to query a stolen gun file. The IGQ and FGQ message keys are now available through the Kansas Central Message Switch. These two message keys can be found under the NLETS INTERPOL Queries folder on the forms tree for OpenFox Messenger users. You may submit a gun serial number via the IGQ as an initial check. A positive response will include the Interpol ID number. The FGQ will provide the full record report when the Interpol ID number is included. For more information on the Interpol Gun Query and other Interpol related requests visit the Nlets Wiki page, <http://wiki.nlets.org>

ADO Field Clarity for NCIC Wanted Person File

A very sharp eyed colleague of ours punctiliously pointed out a conflict with the wording of the NCIC manual for the Wanted Person file. The NCIC 2000 Manual states the following in section 2.5 Additional Guidelines for Entry of the Wanted Person file. "The ADO Field should be used to indicate that multiple WARRANTS exist for the same individual by the same ORI. Additional OFFENSES should be listed in the MIS field." However, when the return of a Wanted Person record includes the ADO information it states "This subject has multiple WARRANTS from this agency." To help alleviate confusion, KBI Help Desk has changed the wording on the form to Additional Warrants (ADO). NCIC determines the field names so the ADO cannot be changed.

FMCSA PRISM Data Now Available in Real Time via Nlets

Federal Motor Carrier Safety Administration (FMCSA) data is available in real time through the Kansas Central Message Switch via Performance and Registration Information Systems Management (PRISM) powered by The International Justice and Public Safety Network (Nlets). Nlets Director Kurt Anzelmo describes this effort in an announcement to Nlets representatives as PRISM cooperatively allows state registration and law enforcement personnel to identify motor carriers and their vehicles who had their registrations suspended or revoked. These identities are housed in the Motor Carrier Safety Improvement Process (MCSIP). Nlets new FMCSA web service allows state registration, law enforcement as well as inspection personnel to query the data housed by MCSIP via two existing message keys. The ACQ and AVQ queries will remain the same except for the additional MCSIP data returned will now be real-time. This eliminates the potential for discrepancies due to outdated information. An additional benefit is users can query by vehicle if the carrier to which it is assigned is "Targeted for Inspection" due to a Federal Out-of-Service Order. Registration personnel can deny vehicle registration to carriers with suspended or revoked registrations. Enforcement officers can inspect these vehicles entered into MCSIP more frequently. Visit the Nlets wiki page for more information about ACQ, AVQ, FMCSA, PRISM, MCSIP and other Nlets resources.

Apportioned Tag Query

Tip: When you query apportioned tags and you do not receive valid data by LIC only, try adding the LIY with current year minus 1. Example: if the current year is 2016 try LIC plus LIY = 2015. Also, if you are using the KCS form, make sure the LIT has the code 'AP'.

KCJIS User Group

At the March meeting the group received information on the Kansas Incident Based Reporting System (KIBRS) from the KBI Information Services Division. Our next meeting is on July 7, 2016 starting at 12:00PM in the Auditorium at the KBI Headquarters building in Topeka.



Java 8 Update 71

Java 8 Update 71 is now available for download via the [CPI Desktop Website](#)

KANSAS OFFENDER REGISTRATION FORM Q&A

JENNIFER SLAGLE, PROGRAM CONSULTANT I KBI

Q. Can the offender registration form be post-dated?

A. No, the registration form must be dated with the actual date the offender signs the registration form.

Q. What information should be listed for tattoos?

A. A location and description of all tattoos should be listed. If a tattoo is covered up or has been removed, that should be noted as well.

Q. Do offenders need to fill out a registration form when they are booked in or out of jail?

A. Registration forms can be filled out, but this type of updated information can also be made with a non-registration edit in KsORT or by notifying your regional contact via email. Offenders need to provide an address when they are released from jail. Accurate dates and current locations are a big help in keeping track of offenders and records up to date.

Q. What if there is more than one address for an employer? Which address should be listed?

A. The employment address should be where the offender is physically working. If the company has headquarters at one location but the offender works at a secondary location, list the secondary location where the offender is actually working.

A. If the offender is self-employed, list the offender's home address as the employment address.

A. If the offender is working for a temp agency and working at locations long-term, list the locations the offender is actually working at. However if the offender is working at a different location every day, list the temp agency.

Q. Should online schools be listed on the registration form?

A. No, only schools where offenders are attending at a physical location should be listed.

Q. What information is needed under internet information?

A. Offender email addresses plus any accounts such as Facebook, Twitter, Snapchat, etc. that the account may be associated with.

Q. What if there isn't enough space on the registration form?

A. There are supplemental sheets available if extra space is needed for the following sections: aliases, scars/marks/tattoos, vehicles, addresses, employment, email addresses, and offenses.

Some final tips »

- » If there is old information on a registration form that is no longer valid, remove it so it doesn't continue to print on current forms.
- » Be sure to have the offender review and sign the registration form and acknowledgement form. And then have both forms signed by a witness as well.
- » The more information we have, the better we are able to protect the public's safety.

If you have any questions about the Kansas Offender Registration Form or any registration issue, please contact the KBI Offender Registration Unit by phone at (785) 296-2841 or by email at registeredoffender@kbi.state.ks.us.

INVOLUNTARY COMMITMENT INFORMATION

GINNY EARDLEY, NICS COORDINATOR KBI

Involuntary commitment orders are to be sent to the Kansas Bureau of Investigation (KBI) central repository as per K.S.A. 75-7c25. An involuntary commitment is a lifetime federal prohibitor for purchasing firearms or explosives.


Once the KBI receives a copy of the involuntary commitment orders the information is electronically submitted to the Federal Bureau of Investigation (FBI) National Instant Background Check System (NICS) Index. The NICS Index along with criminal history found in the National Crime Information Center (NCIC) and the Interstate Identification Index (III) are used to determine if prospective purchasers are disqualified from receiving firearms or explosives.

**INVOLUNTARY COMMITMENT INFORMATION, CONTINUED
GINNY EARDLEY, NICS COORDINATOR KBI**

Medical or mental evaluations should not be submitted to the KBI, as this potentially violates HIPPA laws. When sending Involuntary Commitment information to the KBI, it is crucial to attach a cover sheet detailing the identifiers for the individual. This helps with locating the correct criminal record and limits the amount of follow up contact from KBI to obtain information timely. Please include full name, date of birth, race, gender and any other identifiers that will assist in updating our records accurately.

If questions arise please contact NICS Coordinator, Ginny Eardley at 785-296-8244.

**KCJIS CONFERENCE
AMY JOHNSON, CJIS UNIT KHP**

	<p>KCJIS Conference 2016</p>
<p>CONFERENCE REGISTRATION LINK: https://www.kansas.gov/ssrv-kanpayxpr/services/8555/KFKC-JIS725/additionalInformation.html</p>	
<p>Sunday- June 5, 2016</p>	
<p>5:30 Evening Reception</p>	
<p>Monday- June 6, 2016 beginning at 8am</p>	
<p>Break out topics:</p>	<p>Atrium Hotel & Conference Center 1400 N. Lorraine Hutchison, KS 620-669-9311</p>
<ul style="list-style-type: none"> Open Records NCS-X (NIBRS enhanced) Situational Awareness Open Fox Moto Bridge KS Statewide Interoperable Communication System Electronic Dispositions Archive Retrieval & Configurator NLETS Messenger 3.0 	<p>Rooms Blocked have been blocked at the state rate of \$77</p>
<p>Dinner Provided</p>	
<p>Tuesday- June 7, 2016 beginning at 8am</p>	
<p>Break out topics:</p>	
<ul style="list-style-type: none"> Terrorism: Local & Domestic Radicalization NCIC Violent Person & Investigative Interest Files NORA KORA Sex Offender Audit Standards Cloud Security V5.5 CJIS Security Policy KACIS KCJIS Web Portal Messenger 3.0 NICS 	



The KCJIS Newsletter is published by the
Kansas Criminal Justice Coordinating Council

Derek Schmidt
Attorney General
Chair

Sam Brownback
Governor
Vice-Chair

Council Members

Kirk Thompson
Director
Kansas Bureau of Investigation

Justice Caleb Stegall
Chief Justice Designee

Johnnie Goddard
Interim Secretary
Kansas Department of Corrections

Mark Bruce
Superintendent
Kansas Highway Patrol

Tim Keck
Governor Designee

KCJIS Committee Members

Ed Klumpp
KS Association of Chiefs of Police
Chair

Sec. Sarah Shipman
KS Department of Administration
Vice-Chair

Capt. Lance Royer
KS Sheriffs Association
Treasurer

Leslie Moore
Kansas Bureau of Investigation

Capt. Justin Bramlett
Kansas Highway Patrol

Harold Sass
KS Department of Corrections

Kelly O'Brien
Office of Judicial Administration

Pam Moses
KS Association of District Courts

Amber Norris
KS County and District Attorney Association

Bill Duggan
Lyon CO ECC
KS Assoc. of Public Communications Officers

KANSAS BUREAU OF INVESTIGATION

Jessica Crowder
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
(785) 296-8338
Jessica.Crowder@KBI.STATE.KS.US