



## Article Archives

Looking for a news article that was once posted to the News & Information portion of the Kansas Highway Patrol CJIS Launch Pad? It may be in this collection of archived articles.

**Click on a title or date to view a news article that was previously posted.**

Article Title	Article Date
<a href="#">IC3 alert warning for law enforcement personnel</a>	<a href="#">November 20, 2015</a>
<a href="#">Survey for non-criminal justice personnel with access to CJIS</a>	<a href="#">October 12, 2015</a>
<a href="#">Security Reminder</a>	<a href="#">August 10, 2015</a>
<a href="#">WINDOWS 10 NOTICE</a>	<a href="#">July 28, 2015</a>
<a href="#">Ransomware continues to be a threat</a>	<a href="#">July 14, 2015</a>
<a href="#">Revised KCJIS Policies and Procedures Manual Approved</a>	<a href="#">April 20, 2015</a>
<a href="#">FBI Releases "Ransomware on the Rise"</a>	<a href="#">January 23, 2015</a>
<a href="#">NCIC &amp; Kansas Warrant Entry Worksheets</a>	<a href="#">April 23, 2014</a>
<a href="#">Presentations and Documents updated for 2014</a>	<a href="#">January 15, 2014</a>

Last Archived December 7, 2015



## Article Archives

### **IC3 alert warning for law enforcement personnel November 20, 2015**

*The (FBI) Internet Crime Complaint Center (IC3) has issued an alert warning that law enforcement personnel and public officials may be at an increased risk of cyber-attacks.* In addition to doxing (the act of gathering and publishing individuals' personal information without permission), threat actors have been observed compromising the email accounts of officers and officials. These target groups should protect their online presence and exposure. Users are encouraged to review the IC3 Alert <http://www.ic3.gov/media/2015/151118.aspx> for details and recommended security measures.

### **Survey for non-criminal justice personnel with access to CJI October 12, 2015**

The Kansas Highway Patrol CJIS Unit would like your help to get a better understanding about how many Non-Criminal Justice organizations and personnel (City/County I.T. Departments and private contractors) are being utilized by the KCJIS community in support of the administration of criminal justice in Kansas.

To that end, we have placed a small survey form on the KHP CJIS Launch Pad until November 11, 2015. Follow this link to the survey:

[https://cjisaudit.khp.ks.gov/launchpad/cjisdocs/files/sept\\_2015\\_contract\\_vendor\\_survey\\_distributed.pdf](https://cjisaudit.khp.ks.gov/launchpad/cjisdocs/files/sept_2015_contract_vendor_survey_distributed.pdf)

While this is optional, your participation will help us get a better, bigger picture of how the KCJIS community utilizes non-criminal justice personnel.

The survey forms has space to share about up to 4 departments or companies your agency uses in support of administration of criminal justice. You may complete as many surveys as you need to let us know about all your non-criminal justice relationships.

We thank you in advance for your time

[Back to Page 1](#)

## Article Archives

### Security Reminder      August 10, 2015

This is a reminder that FBI and KCJIS Policy 5.10.4.4 requires the receipt of information system security alerts/advisories on a regular basis. The U.S. Department of Homeland Security's US Computer Emergency Readiness Team (USCERT) website is one resource that helps fulfill this requirement. You can sign up for alerts and advisories here: <https://www.us-cert.gov/ncas>. Receiving these alerts will help to make you aware of zero-day vulnerabilities, such as the recent one in Mozilla's Firefox browser.

Mozilla has issued an emergency update to Firefox version 39.0.3 to patch a serious vulnerability.

You can find the download at: <https://www.mozilla.org/en-US/firefox/new/?scene=2#download-fx>

Knowledge of 0-day attacks and taking preventative measures will help mitigate damage to information systems and reduce security threats.

It will also help to maintain compliance with KCJIS Policy 5.10.4.1 (Patch Management), which requires the identification of applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws, as well as the subsequent patching / updating to address those vulnerabilities.

To keep systems secure, it is critical that they are fully patched. Research shows that over 80% of the reported vulnerabilities are in 3rd-party applications. Operating systems are only responsible for 13% of vulnerabilities and hardware devices for 4%. Based on historical vulnerabilities, it is especially important to focus on patching operating systems (Windows, Linux, OS X), web browsers, Java, and Adobe free products, such as Flash Player, Reader, Shockwave Player, AIR. (<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>)

[Back to Page 1](#)

## Article Archives

### WINDOWS 10 NOTICE July 28, 2015

EVEN THOUGH MICROSOFT HAS ANNOUNCED THAT WINDOWS 10 IS NOW AVAILABLE FOR DOWNLOAD AND UPGRADE FOR CERTAIN DEVICES.

#### **DO NOT INSTALL WINDOWS 10 ON KCJIS ACCESS DEVICES UNTIL FURTHER NOTICE.**

THE KBI HELPDESK CANNOT SUPPORT WINDOWS 10 AT THIS TIME.

AS WITH ANY NEW OPERATING SYSTEM, IT MAY CONTAIN BUGS, VULNERABILITIES OR NEW PROGRAM CODE THAT IS INCOMPATIBLE WITH YOUR APPLICATIONS.

FOR INSTANCE IT INCLUDES A NEW INTERNET BROWSER.

AN INTEGRAL PART OF PATCH MANAGEMENT POLICY 5.10.4.1 IS TESTING.

THE KBI AND OUR VENDORS HAVE NOT HAD THE OPPORTUNITY TO THOROUGHLY TEST WINDOWS 10 AND MAKE ADJUSTMENTS TO ENSURE COMPATIBILITY WITHOUT OPENING VULNERABILITIES.

FOR WHAT OPERATING SYSTEMS ARE SUPPORTED BY KBI HELPDESK, REFER TO THE KCJIS COMPUTER SPECIFICATIONS DOCUMENT AVAILABLE ON THE KCJIS SECURE WEB PORTAL (TOKEN ACCESS) AT [HTTPS://WWW.KCJIS.STATE.KS.US/SITEPAGES/KCJIS\\_HOME.ASPX](https://www.kcjis.state.ks.us/sitepages/kcjis_home.aspx) CLICK INFORMATION ON THE MENU BAR THEN SCROLL TO THE KS TECHNICAL INFORMATION SECTION TO LOCATE THE DOCUMENT.

### Ransomware continues to be a threat July 14, 2015

The upcoming issue of the KCJIS newsletter is scheduled to contain an article with a reprint of a June 23, 2015 Security Alert from the FBI's IC3 that has updated information about CRYPTOWALL, a form of RANSOMWARE that is still very active. Click [HERE](#) for a preview of that article.

[Back to Page 1](#)



## Article Archives

### Revised KCJIS Policies and Procedures Manual Approved April 20, 2015

On Monday, April 13, 2015, the KCJIS Committee approved a revised KCJIS Policies and Procedures manual after a few minor corrections. Those corrections have been made and the revised policy is now available from the CJIS Documents area of the Kansas Highway Patrol CJIS Launch Pad . It can also be found within the CJIS manual area of the Launch pad or under the **Information** Menu in the KCJIS Secure Web Portal by scrolling down to the Security Policies

### FBI Releases "Ransomware on the Rise" January 23, 2015

The FBI has released an article addressing ransomware campaigns that use intimidating messages claiming to be from the FBI or other government agencies. Scam operators use ransomware – a type of malicious software – to infect a computer and restrict access to it until a ransom is paid to unlock it. Users and administrators are encouraged to review the FBI article "Ransomware on the Rise" for details and refer to Alert TA-295A for information on Crypto Ransomware.

### NCIC & Kansas Warrant Entry Worksheets April 23, 2014

The Kansas Highway Patrol CJIS Unit has once again, created the entry worksheets to be made “ fillable” for NCIC and Kansas Warrant entries.

The worksheets are located on our CJIS Launch Pad. Select CJIS DOCUMENTS, NCIC and finally NCIC Worksheets.

The boxes that are highlighted in red are mandatory fields to enable the entry to be made in OpenFox. Refer to the KCJIS Policy and Procedures and Audit Standards on other mandatory requirements for the entries.

If you have any questions, contact your Data Quality Trainer/Auditor

### Presentations and Documents updated for 2014 January 15, 2014

The PowerPoint training presentations for NCIC (both Full and Limited Access), TAC Administration, TAC Web Portal and National Sex Offender Registration have been replaced on this site with versions updated for calendar year 2014.

In addition, current 2014 versions of both the TAC Manual and Data Quality Audit Standards documents have been posted to replace the previous versions.

[Back to Page 1](#)