
# WISCONSIN

# TIME SYSTEM

# 2023 INSERVICE TRAINING

# Table of Contents

# ***CJIS Security Policy Changes***

The newest update to the CJIS Security Policy was published October 1, 2022. The newest update of the CJIS Security Policy, marks the beginning of the overhaul of the policy. The FBI will be revising and updating the policy section by section as well as adding new sections. These updates will change the format of the policy. The FBI estimates that there will be two policy updates per year while this process is ongoing, with the final update to version 6.0 anticipated for Spring 2025.

This first update focused on modernizing the Media Protection section of the policy. The new format for the policy provides a topic and security controls for the topic in each section detailing the requirements for the topic. This update contains seven controls for Media Protection with requirements for each control. Each control has a discussion section where more information is provided for the control area. The new controls from this policy update will be sanctionable for audit beginning October 1, 2023.

**MP-1 Policies and Procedures**: Agencies are already required to have policies relating to media protection. The update requires that agencies develop procedures to facilitate the implementation of the media protection policy and the associated media protection controls. An individual with security responsibilities must be designated to manage the development, documentation, and dissemination of the media protection policies and procedures. These policies and procedures are to be reviewed and updated at least annually and following any security incidents involving digital and/or non-digital media.

**MP-2 Media Access**: Agencies will continue to restrict access to digital and non-digital media to authorized individuals. An Authorized User is someone who has passed a fingerprint-based background check, completed Security Awareness Training, and appears on your agency's Authorized User List.

**MP-3 Media Marking**: A new requirement, media marking requires agencies mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Digital or non-digital media containing CJI remaining in the physically secure location is exempt from the media marking requirement.

**MP-4 Media Storage**: Agencies will continue to physically control and securely store digital and non-digital media within the physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible. Agencies will also protect system media types where CJI is encrypted on digital media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

**MP-5 Media Transport**: Agencies will continue to protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the

physically secure location or controlled areas. Physical media will be protected at the same level as the information would be protected in electronic form. Agencies will restrict the activities associated with transport of electronic and physical media to authorized personnel. A new requirement with this update is that agencies will maintain accountability for system media during transport outside the physically secure location or controlled areas and document activities associated with the transport of system media. Agencies will continue to restrict activities associated with the transport of system media to authorized personnel only.

**MP-6 Media Sanitization**: Agencies will continue to sanitize or destroy digital and non-digital media prior to disposal, release from agency control, or release for reuse using an overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable media will be destroyed and physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration. Agencies will need to employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

**MP-7 Media Use**: A new requirement with this update, agencies will restrict the use of digital and non-digital media on agency owned systems that store, process, transmit CJI by using technical, physical, or administrative controls. Agencies will prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CJI. Agencies will prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.

Version 5.9.1 also updated the language for Section 5.12 Personnel Security and provides clarification for when a fingerprint-based background check should be done. The policy clarifies that the fingerprint check should be done for **unescorted access** to unencrypted Criminal Justice Information (CJI)—either physical or logical access. A new guideline was added for cloud provider personnel. If the cloud provider personnel do not have access to unencrypted CJI, a fingerprint-based record check may not be required.

The last update in Version 5.9.1 is updates to Appendix G.3 for Cloud Computing. The updates remind agencies that the CJIS Security Policy sets the **minimum** requirements for the protection of CJI. Additional security assurances may be leveraged but it does not guarantee they meet the requirements of the CJIS Security Policy. Agencies should be cautious and ensure any cloud provider they utilize is meeting the requirements of the policy.

Appendix G.3 also updated the language for Service Models and helps clarify that the way CJI is placed and accessed in the cloud determines if the personnel security requirements from Section 5.12 apply. If you use a Cloud Provider, please review

Appendix G.3 to determine which service model your agency uses and ensure you are meeting the requirements based on your service model.

The CJIS Security Policy can be found on the FBI website in its most current form. If you have any questions regarding the policy or its updates, please contact CIBTrain@doj.state.wi.us.

# ***$.H.U21 NICS Under 21 Attempt to Purchase Firearm***

On Monday, November 14, 2022, the National Instant Background Check System (NICS) Section of the FBI began conducting additional outreach for background checks conducted by NICS initiated at a federal firearms licensee when the potential firearm transferee is under the age of 21. This outreach is to determine if the person has juvenile criminal/delinquency information or juvenile mental health adjudications/commitments that may be disqualifying for the receipt or possession of firearms under federal law.

In such an event, NICS will contact the state criminal history repository (the Crime Information Bureau in Wisconsin) or juvenile justice information system, as well as the appropriate state custodian of mental health adjudication information in which the person resides requesting the relevant juvenile information. Outreach will be conducted through the established method as directed by the individual agency (i.e. email).

Additionally, the new legislation also requires the NICS Section to contact the local law enforcement agencies of the jurisdiction where the person resides. When a NICS check is initiated for a potential firearm transferee under the age of 21, the NICS Section will send a $.H.U21 unsolicited message via the TIME System to the local agency based on the contact information provided by the individual to the firearms dealer. If your agency does not have a TIME System terminal, the message will be sent to the county's TIME System terminal designated for your agency.

If your agency receives a request for potential juvenile information from the NICS Section, you are requested to reply within three business days. If a search of your agency's records results in no relevant information, your agency should still send a response advising of no records to the NICS Section. Agencies are also asked to provide information on other potentially applicable federal, state, tribal, or local firearm prohibitions including information establishing the potential firearm transferee as a current user of controlled substance, or a respondent of a protection order, etc.

It should be noted that while these messages include a request for relevant juvenile mental health records, Wisconsin already reports juvenile mental health adjudications/commitments with a firearm restriction to the NICS Section for inclusion in the NICS Indices.

Any information shared with the NICS Section will only be used for approved NICS purposes.

Example of Request for Potential Juvenile Information:

**********

In accordance with the Bipartisan Safer Communities Act, when individuals under 21 years of age seek the transfer of a firearm through a federal firearms licensee, the FBI's National Instant Criminal Background Check System (NICS) Section is required to contact your agency for information. We are primarily reaching out to you seeking relevant *juvenile* information on the subject below. However, if you have knowledge of or possess *any* information that could impact the subject's eligibility to receive a firearm, we request you provide such information as well or make us aware by emailing NICS_U21@fbi.gov.

Please respond to this request within three business days, including the NICS Transaction Number (NTN) listed below. Please indicate whether your agency does/does not possess prohibiting information or whether your agency has knowledge of potentially prohibiting information.

Name Last, First M NTN

Sex

Race

Date of Birth

Place of Birth

Height Weight

Social Security Number

Residence Address:

The types of information you may possess include, but are not limited to, an inference of drug use within the past year, active warrants, active protection orders, pending or convicted criminal cases, or mental health adjudications. If a mental health adjudication is located and cannot be shared directly with the NICS Section, please indicate this in your email response. If you have questions regarding this request, please provide a name and phone number and the NICS Section will contact your agency for further discussion.

*Please note (in regards to mental health adjudications): The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, Title 45, Code of Federal Regulations, section 164.512(k)(7), was amended in 2016 (81 Federal Register 382-01) to allow covered entities to disclose protected health information to the NICS without requiring the individual's consent, in order to report the identities of individuals who are prohibited from shipping, transporting, possessing, or receiving a firearm based on the federal "mental health prohibitor," Title 18, United States Code, section 922(g)(4).*

**********

The NICS Section is available at 844-265-6716 or NICSLiaison@fbi.gov to assist agencies with questions regarding firearm prohibitions and/or discuss methods of making information available to NICS.

# ***$.H.NDN NICS Denied Notification***

Beginning on September 26, 2022, agencies might have seen a new unsolicited "$" message from NCIC. This new unsolicited message, $.H.NDN, is a NICS Denial Notification.

These notifications are sent to agencies when an individual is denied the purchase of a firearm by NICS within an agency's jurisdiction. The unsolicited message will be sent to the agency's main terminal informing them of the denial. The message will include the name, demographic information of the individual who was denied, the reason for the denial, and where the attempted purchase was made.

It is at the agency's discretion to determine if action needs to be taken based on the message. Here is a sample message:

**********

FIREARM DENIAL NOTICE:
A PERSON PURCHASING/RESIDING IN YOUR JURISDICTION WAS RECENTLY DENIED THE TRANSFER OF HANDGUN

**********

THE FBI ENCOURAGES YOU TO CONTACT YOUR LOCAL BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES OFFICE PRIOR TO TAKING ACTION. CHARLESTON ATF, 304-234-5678

THENATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) SECTION CONDUCTED A NAME SEARCH USING DESCRIPTIVE DATA, NOT FINGERPRINTS, FOR A FIREARM BACKGROUND CHECK WHICH WAS DENIED ON 4/26/2022, 02:02:23PM FOR:
NAME: DOE, JOHN L. NTN: 102356748
SEX: M RACE: W DATE OF BIRTH: 10-11-1990 PLACE OF BIRTH: WV
HEIGHT: 6'1'' WEIGHT: 185 SOCIAL SECURITY NUMBER: 123-45-6789
RESIDENCE ADDRESS: 456 AMERICAN WAY, APPLE PIE, APPLE PIE COUNTY, WV 22445
INFORMATION RECEIVED INDICATES THE ATTEMPTED PURCHASER IS PROHIBITED FROM RECEIVING OR POSSESSING FIREARMS IN THE STATE OF PURCHASE AND/OR STATE OR RESIDENCE, BASED ON:
SUBJECT OF QUALIFYING PROTECTION ORDER
THE ATTEMPTED PURCHASE OCCURRED AT:
FIREARM DEALER: USA ARMS
ADDRESS: 123 MAIN STREET, HOMETOWN, HOMETOWN COUNTY WV, 23456
PHONE: 304-625-1002
SHOULD YOU HAVE QUESTIONS REGARDING THIS NOTIFICATION, PLEASE VISIT: (Web address will be inserted when established WWW.FBI.GOV)
THIS NOTIFICATION WAS ALSO PROVIDED TO THE FOLLOWING ORI(S):
WV0470150 SO APPLE PIE COUNTY 304-478-0000
WV0625630 PD HOMETOWN 304-457-0000

# ***"Kayleigh's Law"***

A new law has passed in Wisconsin that allows for the entry of permanent or non-expiring protection orders for victims of sexual assault. Kayleigh's Law was made into law with 2021 Wisconsin Act 256. Kayleigh's Law amends portions of law that govern the expiration limits of injunctions.

The victim may request that a protection order be issued permanently to ensure the victim will not have to face their abuser again. This law is applicable for domestic abuse injunctions, child abuse injunctions, individuals at risk (vulnerable adult) injunctions, and harassment injunctions.

Currently, the TIME System does not allow entry of a non-expiring protection order. In order to enter these new permanent non-expiring protection orders, agencies should enter the expiration date of December 31, 2150. Agencies may also include in the MIS Remarks that the protection order is non-expiring.

# ***N-DEx***

What is N-DEx? The N-DEx System is an unclassified national strategic investigative information sharing system bringing together records from across the nation. The National Data Exchange System provides access to nearly one billion searchable records from over 8,100 criminal justice entities sharing information nationwide. N-DEx provides the criminal justice community an opportunity to connect, search, share, and analyze millions of records with one search. N-DEx records span the criminal justice life cycle and include, but are not limited to incident case reports, arrests, missing person reports, booking and incarceration reports, probation and parole reports, warrants, citations, tickets, field contact interviews, service calls, etc.

N-DEx can assist investigators to determine relationships between people (subjects/ victims/witnesses), things (vehicles/property), locations and characteristics of a crime to provide valuable leads. Federal data available via the N-DEx System includes records from the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), International Criminal Police Organization (INTERPOL), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Marshals Service (USMS), Federal Bureau of Prisons (BOP), Transportation Security Administration (TSA), Federal Air Marshal Service (FAMS), Joint Automated Booking System (JABS), and the Department of Defense (DoD). N-DEx tools include Batch Search functions, which enable users to search thousands of people, phone numbers, or vehicles at one time. The Subscription and Notification tool provides

users with automatic notifications when a subject has an encounter with another law enforcement agency. Visualization tools are available, which allow users to graphically display associations on a link analysis chart or map, to support predictive policing.

Contributing to N-DEx is highly recommended to law enforcement agencies across the country. Enrolling in N-DEx can provide your agency with benefits such as increasing officer safety by preparing officers for encounters by providing a snapshot of an encountered persons criminal records, photographs, and associations in an easy to-read format. N-DEx can also be a powerful tool for corrections agencies by improving case management, providing supplementary information for visitor screening, and allows for more effective client monitoring of individuals on probation.

Data contributed to N-DEx may be formatted via Secure File Transfer Protocol (SFTP) over the public internet to submit records. The SFTP method is the preferred method for submission of large batches of data to the N-DEx System. Web service submission is used to extract, transform, and submit data in real-time. Web Service connections are preferred over the public internet. The FBI N-DEx office can provide No-cost technical assistance to agencies interested in making their data available in the N-DEx System, but do not have the necessary technical resources. Agencies that are interested in contributing to N-DEx may contact CIB for more info at cibtrain@doj.state.wi.us or contact N-DEx directly at ndex@leo.gov. To access N-DEx, users must have a LEEP account. Visit www.cjis.gov to complete a LEEP access form.