



U.S. Department of Justice

Federal Bureau of Investigation

Clarksburg, WV 26306

January 30, 2016

TO: ALL CJIS SYSTEMS OFFICERS (CSOs)

The purpose of this letter is to provide you with the newly established policies, procedures, and implementation guidelines applicable when law enforcement and criminal justice agencies use National Crime Information Center (NCIC) data for site access to Critical Infrastructure Facilities (CIFs).

Protection of our nation's key assets has been an area of concern for law enforcement for many years. In 2008, the Criminal Justice Information Services (CJIS) Division's Joint Advisory Policy Board and National Crime Prevention and Privacy Compact Site Security Task Force maintained that accessing NCIC (hot file) data for screening visitors to CIFs by law enforcement agencies is an authorized use of the information. In the fall of 2014, this issue was again addressed through the CJIS Advisory Process, primarily to provide clarity on the use of specific NCIC files (now deemed restricted and nonrestricted) for this purpose and to establish universally acceptable practices related to the sharing of disqualifying and non-disqualifying results obtained from NCIC information with CIF personnel. The NCIC restricted files are defined in the *CJIS Security Policy, Section 4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information*. It is important to note that the NCIC restricted files do not include criminal history record information.

The new CIF visitor screening policies, procedures, and implementation guidelines outlined below were approved by the CJIS Advisory Policy Board (APB) in December 2014 and subsequently the Director of the Federal Bureau of Investigation (FBI).

CIF Visitor Screening Policies and Procedures

1. The FBI, in conjunction with the CSOs, should take specific action to educate criminal justice agencies on their existing authority to conduct NCIC restricted and nonrestricted file checks on visitors to critical infrastructure facilities and that no additional authority is needed to allow such checks.

ALL CJIS SYSTEMS OFFICERS (CSOs)

2. The CJIS System Agencies (CSAs) and/or their respective jurisdictions will determine what constitutes a visitor for NCIC purposes.
3. The CSAs and/or their respective jurisdictions will determine what constitutes a CIF for NCIC purposes.
4. Nondisqualifying notifications may be automatically sent to the CIF as mutually agreed upon by the involved entities. Potential disqualifiers will be reviewed by the law enforcement agency which may elect to notify the CIF of a pending review.
5. Redress procedures must be made available to individuals who are subjected to NCIC checks resulting in denied CIF facility access from either the partnering law enforcement agency or CIF. The CIF shall direct redress requests associated with NCIC checks to the partnering law enforcement agency.
6. Contractor personnel conducting the screening do not need to meet the CJIS audit requirement according to the *CJIS Security Policy, Section 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum*.

CIF Visitor Screening Implementation Requirements

The CJIS Division provides the following implementation requirements for screening visitors to CIFs, which are necessary and may be assessed during CJIS Division audits:

1. Any law enforcement agency wishing to participate in screening visitor access for a CIF shall request, through their CSA, a unique NCIC Originating Agency Identifier (ORI) from the FBI's CJIS Division. The ORI can be requested by contacting the NCIC Operations and Policy Unit (NOPU) via:
 - A. United States mail at Federal Bureau of Investigation, Criminal Justice Information Services Division, NCIC Operations and Policy Unit, Module D3, 1000 Custer Hollow Road, Clarksburg, WV 26306, Attention: Systems Access;
 - B. Electronic mail at <ori@leo.gov>; or
 - C. Facsimile at (304) 625-2924.
2. Law enforcement agencies shall be responsible for ensuring that CIF screening is conducted based on agreed-upon standards and not conducted on employees as an alternative method of a background check.

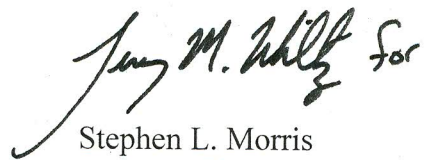
ALL CJIS SYSTEMS OFFICERS (CSOs)

3. A memorandum of understanding (MOU) shall be established among the responsible law enforcement agency, the CIF, and any third party involved to assist with the routing of messages between the law enforcement agency and the CIF. The MOU shall:
 - A. Clearly articulate redress procedures.
 - B. Identify which NCIC files will be used for disqualification into the CIF.

The CIF visitor screening policies, procedures, and implementation guidelines were effective as of October 28, 2015. If you have any questions regarding the use of NCIC data for access to CIFs, please contact your respective NOPU Regional Representative listed below.

Region	NOPU Representative	Phone	E-mail
Federal	Gary E. Davis	(304) 625-4583	<gary.davis@ic.fbi.gov>
Northeastern	Richard Dion Bright	(304) 625-7327	<richard.bright@ic.fbi.gov >
Western	Zachary P. Hartzell	(304) 625-4718	<zachary.hartzell@ic.fbi.gov>
Southern	Patsy T. Sabatelli	(304) 625-5499	<patsy.sabatelli@ic.fbi.gov>
North Central	Nick L. Barron	(304) 625-4411	<nick.barron@ic.fbi.gov>

Sincerely yours,



Stephen L. Morris
Assistant Director
Criminal Justice Information
Services Division