General Order

Houston Police Department

ISSUE DATE:	NO.
April 20, 2021	800-06

REFERENCE: Supersedes all prior conflicting Circulars and Directives, and General Order 800-06, dated October 9, 2014

SUBJECT: CJIS COMPLIANCE

POLICY

The Houston Police Department (HPD) shall comply with state and federal criminal justice information services (CJIS) regulatory policies associated with the protection and access controls of criminal justice information (CJI) as defined in this General Order.

This General Order applies to all employees.

DEFINITIONS

CJIS Compliance Unit (CCU). The HPD unit assigned to the Risk Management Division that administers policy regulations to ensure the department maintains state and federal operational compliance associated with the protection of CJI.

CJIS Compliance Verification Database. An HPD database that employees may use to view the CJIS compliance status of *non-HPD personnel* as determined by the *CJIS Compliance Unit*. The database is populated and maintained by the CJIS Compliance Unit and is accessible via the department's Intranet Portal.

CJIS Security Policy (CSP). A policy approved and published by the Federal Bureau of Investigation (FBI) and that contains the minimum information security requirements, guidelines, and agreements for protecting the sources, generation, transmission, storage, and destruction of CJI. The *CJIS Security Policy* is available on the department's Intranet Portal.

Contractor. A private business, agency, or individual that has entered into an agreement with HPD or the City of Houston to conduct services or provide specific products for the department.

Criminal History Record Information. A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person and that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Information (CJI). For the purposes of this General Order, *criminal justice information* refers to any and all of the criminal justice data necessary for law enforcement agencies to perform their mission. Such data includes, but is not limited to, biometric, identity history, person, organization, property, and case/incident history data as well as *criminal history record information.*

Criminal Justice Information Services (CJIS) Division. The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Escort. Authorized personnel who accompany a visitor or other *non-HPD personnel* who have not been approved by the CJIS Compliance Unit (CCU) for *unescorted physical access*. *Escorts* shall accompany such persons at all times while in a *physically secure location* to ensure the protection and integrity of the *physically secure location* and any *criminal justice information* accessible therein. All HPD employees are authorized and required to provide *escort* to a visitor or other *non-HPD personnel* who have not been approved by the CCU for *unescorted* physical access into secured areas under the management control of HPD.

Escorted. Refers to the status of persons who have or require an *escort* to enter a *physically secure location*. CCU approval for *escorted access* is available for only *physical access*, not *logical access*.

Local Agency Security Officer (LASO). The employee who serves as the primary information security contact between HPD and the Texas Department of Public Safety through which HPD interfaces with the FBI CJIS Division.

Logical Access. The ability, right, or privilege of an individual or technological process to utilize or access (including remotely) any HPD technology system or application via technological, electronic, or computerized means.

Non-HPD Personnel. Any person conducting services at HPD and not paid directly through HPD's payroll (e.g., *contractors*, volunteers, external agency personnel, temporary workers, and other government personnel). For the purposes of this General Order, this term does not include visitors, who shall be *escorted* at all times while in a *physically secure location*.

Personally Identifiable Information (PII). Information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

Physical Access. As used in this General Order, *physical access* refers to the physical ability, right, or privilege to enter a *physically secure location* as defined herein. *Physical access* may be *escorted* or *unescorted*.

Physically Secure Location. A police vehicle or a facility, including an area, a room, or a group of rooms within a facility, under HPD management control where CJI may be accessible and where the public is not allowed access without an *escort* as defined herein or authorization for *unescorted physical access* from the department's CCU.

Terminal Agency Coordinator (TAC). The employee who serves as the point of contact between HPD and the Texas Department of Public Safety for matters relating to accessing the Texas or National Crime Information Centers (TCIC/NCIC), Texas Law Enforcement Telecommunications System (TLETS), or other CJI as defined herein. The TAC is assigned to the CCU.

Unescorted. Refers to the status of persons who do not have or do not require an *escort* to enter a *physically secure location*. Unless otherwise excluded, all HPD employees and *non-HPD personnel* who are approved by the CCU for *unescorted physical access* are authorized to enter a *physically secure location unescorted*.

1 DUTIES AND RESPONSIBILITIES

Executive Assistant Chiefs and Assistant Chiefs

Executive assistant chiefs and assistant chiefs shall help promote CJIS compliance and policy development to ensure HPD's information technology advancements meet or exceed the minimum access controls as required by the latest state and federal CJIS security policies.

Division Commanders

Division commanders are responsible for ensuring that all *non-HPD personnel* allowed *escorted* or *unescorted physical access* to a location under their management control are approved for such access by the Risk Management Division, *CJIS Compliance Unit* (CCU). Verification shall be made through the *CJIS Compliance Verification Database* via the department's Intranet Portal or by direct inquiry to the Risk Management Division, CCU. For information regarding *physical access* for non-HPD law enforcement officers, see section 5 of this General Order.

Division commanders shall verify the *logical access* status for *non-HPD personnel* by first contacting the CCU.

Supervisors

Supervisors must ensure their subordinates maintain CJIS compliance to access *criminal justice information* (CJI) by completing the annual *Employee Integrity and Verifications Program* checks and remind their subordinates to complete their required recertification tests. See General Order 200-11, **Employee Integrity and Verifications Program**. In the event an employee's criminal history record is returned and found to be non-compliant according to the *Texas CJIS Systems Access Policy*, the supervisor shall contact HPD's Internal Affairs Division to ascertain the proper course of action.

Risk Management Division CJIS Compliance Unit (CCU)

The CCU ensures HPD employees are apprised of the minimal security guidelines and regulations established by the FBI *CJIS Security Policy* and the *Texas CJIS Systems Access Policy*. The CCU disseminates educational and advisory updates related to CJIS operational compliance to department employees and makes recommendations upon request regarding CJIS policy conformity involving specific equipment used to connect to HPD's computer network. The CCU does not directly approve or disapprove implementation of any operational objective.

Employees shall contact the CCU to vet all *non-HPD personnel* needing either *logical access* or *escorted* or *unescorted physical access* as defined herein.

The *terminal agency coordinator* (TAC) oversees HPD's compliance with CJIS systems policies.

Local Agency Security Officer (LASO)

The *local agency security officer* (LASO) actively represents HPD with CJIS information security audits of hardware and reviews CJIS operational compliance procedures. The LASO assists the

Office of Technology Services with ensuring CJIS security policies are maintained within HPD's technology systems and that state and federal CJIS policy inquiries are resolved. The LASO keeps the Texas CJIS Compliance Office informed regarding information security issues.

Office of Budget and Finance

The Office of Budget and Finance serves as the liaison for processing temporary employees under the citywide contracts with temporary hiring agencies.

The Procurement Section helps facilitate the completion of CJIS agreements with *contractors* who have a need for *logical access* or *physical access*. The Procurement Section also provides guidance when CCU requires other City departments to comply with CJIS requirements on non-HPD contracts. The Procurement Section ensures original signed CJIS Security Addendums for HPD contracts are filed appropriately with the City Controller's Office and HPD.

Office of Community Affairs

The Office of Community Affairs serves as the liaison for processing volunteers and interns who conduct support services for HPD.

The Office of Community Affairs, in conjunction with the CCU, develops and maintains on the department's public website the most updated resource materials to help *contractors* understand HPD CJIS protocols.

Employee Services Division (ESD)

The Employee Services Division is responsible for issuing all identification credentials. *Non-HPD personnel* working *unescorted* in secured areas on a temporary basis may be issued identification credentials when requested by a division commander and approved by the ESD division commander.

Office of Technology Services

The Office of Technology Services serves as the primary resource responsible for HPD technology systems and delivery of related services. The Office of Technology Services works with the CCU to ensure that HPD technology systems are operated and maintained in compliance with CJIS security policies.

2 CJIS SECURITY POLICY

The FBI *CJIS Security Policy* (CSP) contains the minimum information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, generation, transmission, storage, and destruction of CJI.

The state adheres to the CSP and has the authority to implement more stringent security measures. HPD conforms to the state and federal CJIS security policies; however, the Chief of Police has the authority to implement security measures in addition to those implemented by the state. The CSP is considered a living document. The CJIS Compliance Unit shall ensure

that the latest approved version is available to all employees on the department's Intranet Portal.

3 SECURING CRIMINAL JUSTICE INFORMATION

It is the responsibility of every employee to secure CJI in any form (digital, hardcopy, electronic, etc.) from being exposed to unauthorized personnel. Any CJI obtained or maintained by HPD including, but not limited to, education, financial transactions, medical history, or criminal or employment history may include *personally identifiable information* (PII). *Criminal history record information*, for example, inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file. PII shall be extracted from CJI for official business only.

Employees shall ensure no PII is contained in any email sent outside of HPD's computer network, unless contained in an attachment that is encrypted or password protected. The password shall be sent to the recipient in a separate email in order to protect the contents of the attached document.

Employees shall ensure physical and electronic media containing CJI is safeguarded at all times. If media containing CJI becomes inoperable or when it is no longer needed or required per department records retention policies, the media shall be destroyed by shredding or incineration. Employees shall ensure any disposal or destruction of CJI is witnessed or carried out by authorized personnel.

4 LOGICAL ACCESS CONTROLS

When making *logical access* (technological, electronic, or computerized) to any HPD computer or network, all system users shall utilize their assigned user ID and password to log in. Generic passwords shall not be used to access systems attached to the HPD computer network.

Any division requiring *non-HPD personnel* to conduct Texas Law Enforcement Telecommunications System (TLETS) transactions or to access any HPD computer shall first contact the CCU to ensure the person has completed the *Non-HPD Personnel Logical System Access* form and is CJIS compliant. This form is available on the department's public website or Intranet Portal or from the CCU.

Connections to any HPD technology system shall be established with only the equipment and software approved by the HPD Office of Technology Services and the LASO.

Employees shall confer with HPD's Office of Technology Services regarding purchases involving technology items prior to project development and implementation in order to ensure CJIS compliance for the method of use of the specific item. If the Office of Technology Services is not able to ascertain a definitive response, the CCU shall obtain an official approval from the state.

5 PHYSICAL ACCESS CONTROLS

Visitor Access

All facilities under the management control of HPD shall require visitors entering a *physically secure location* to check in at the main entrance to have their identity verified (e.g., by presenting government issued identification). Some buildings have designated public access areas to conduct business or services where *unescorted* visitor access is permitted (e.g., entry lobbies, common hallways, vending areas, lunch rooms, museums, bonding waiting rooms, and some elevator waiting areas). However, once a visitor enters a *physically secure location* the visitor shall be *escorted* at all times by authorized personnel.

Non-HPD Personnel Access

HPD employees shall contact the CCU to process *non-HPD personnel* scheduled to conduct services at a *physically secure location* at least 10 *working days* prior to the job start date. If an immediate need does not allow time for CCU processing, CCU may grant *non-HPD personnel* temporary *physical access* under *escort*. The CCU shall populate the *CJIS Compliance Verification Database* with the *physical access* status (*escorted* or *unescorted*) of all *non-HPD personnel* scheduled to perform services at any *physically secure location*.

HPD employees working security desks at building entry points shall utilize the *CJIS Compliance Verification Database* via the department's Intranet Portal to verify the *physical access* status of any *non-HPD personnel* who does not have an HPD identification card and who is seeking *escorted* or *unescorted physical access* to conduct services at HPD. This includes, but is not limited to, *contractors*, other City of Houston department personnel, volunteers, or interns.

If the *CJIS Compliance Verification Database* is not available or does not return any data regarding an inquiry, the HPD employee shall verify the person's nature of business with the CCU, if available, or the concerned division, or associated City department project manager. The concerned division or authorized personnel from another City department coordinating services shall ensure an *escort* is provided before *physical access* is granted.

Non-HPD Law Enforcement Officers

Unless otherwise excluded, any United States law enforcement officer with a current identification issued from the concerned law enforcement agency is CJIS compliant. However, these officers are subject to the building security policies of the concerned HPD-controlled facility, division, or area.

6 CJIS TRAINING

It is the responsibility of each employee to complete the minimum CJIS training as required by the department in order to access any state or federal *criminal justice information* system. The CCU maintains and tracks all HPD employee online training records and recertification related to the CJIS Compliance mandates. It is the responsibility of the HPD Training Division to maintain and track all HPD employee in person classroom training records related to state and federal mandates.

The CCU along with training coordinators shall provide assistance to employees in order to fulfill required training offered via the Internet (including nexTEST© or CJIS Online). The Texas Department of Public Safety's nexTEST and CJIS Online Training Websites are accessible through any Internet connection.

7 AUDITS

The Houston Police Department undergoes scheduled and unscheduled CJIS information technology compliance audits (see General Order 800-11, **TCIC/NCIC**). The CCU facilitates the preparation and handling of audit interviews along with the concerned divisions. Upon request, divisions shall cooperate with the CCU to help facilitate audit requests. Actionable items in audit findings shall be corrected by the controlling office or division.

8 PENALTIES

Improper access, use, or dissemination of CJI may result in state and federal administrative sanctions against the employee and/or the department including, but not limited to, termination of services and state and federal criminal penalties. Employees may also be subject to departmental disciplinary action up to and including indefinite suspension.

Troy Finner
Chief of Police