ATTACHMENT C

RFP2026-08

(AIA EXHIBIT B)

EXHIBIT(B)

HOOD COUNTY JAIL SECURITY AND ACCESS REQUIREMENTS

1. GENERAL

The existing Hood County Jail will remain operational throughout construction of the Project. The Contractor shall coordinate its Work so that the safety, security, and ongoing operations of the facility are maintained at all times.

The attached **Hood County Jail Sheriff's Office Contractor Access, Security & Construction Operations Directive** establishes the Sheriff's Office requirements and procedures applicable to contractors, subcontractors, vendors, inspectors, delivery personnel, and other individuals performing Work at the Hood County Jail.

The Contractor and all subcontractors shall comply with the attached Directive and all applicable Hood County and Hood County Sheriff's Office security requirements throughout the duration of the Project.

This Exhibit is intended to supplement and reference the attached Directive and identify certain project-specific administrative and CJIS requirements. It is not intended to replace or supersede the Directive.

2. CONTRACTOR RESPONSIBILITY

The Contractor shall be responsible for ensuring that its employees, subcontractors, vendors, suppliers, delivery personnel, and other personnel under its control understand and comply with the applicable security and access requirements for the Project.

The Contractor shall designate a responsible representative to coordinate security and access requirements with Hood County and the Hood County Sheriff's Office.

The Contractor shall be responsible for coordinating required personnel documentation, training, fingerprinting, access approval, and other applicable requirements sufficiently in advance of when access is needed.

3. ACCESS REQUIREMENTS

Access requirements will vary depending on the location and nature of the Work.

The Contractor shall refer to the attached Sheriff's Office Directive for requirements associated with:

- Work outside the secure perimeter.
- Work inside the secure perimeter but outside the existing jail.
- Work within the existing jail or other restricted areas.
- Escorted and unescorted access.
- Daily arrival and departure procedures.
- Emergency access.
- Tools, equipment, materials, vehicles, and deliveries.
- Security systems and controlled areas.
- Jail operations, shutdowns, emergencies, and lockdowns.

Access to any portion of the facility shall be subject to authorization by Hood County and the Hood County Sheriff's Office.

4. CJIS AND PERSONNEL ACCESS REQUIREMENTS

Personnel requiring access to the existing jail shall comply with all applicable CJIS-related requirements established by the Hood County Sheriff's Office and its designated CJIS authority.

The requirements below are part of the overall CJIS and personnel access process and shall be completed as applicable prior to receiving the associated access authorization.

A. CJIS Training

All Contractor and subcontractor personnel who will enter the **existing jail**, whether escorted or unescorted, shall complete required CJIS Security Awareness Training prior to entering the facility.

Personnel who remain outside the existing jail are not required to complete CJIS training unless otherwise directed by the Hood County Sheriff's Office or its designated CJIS authority.

CJIS training is administered through **CJIS Online**. Following award, the Contractor and applicable subcontractors shall coordinate with the Hood County Sheriff's Office to establish the necessary company/vendor accounts and designate an administrator responsible for adding personnel and distributing training assignments.

The training typically takes approximately **15–20 minutes** to complete.

The Contractor shall be responsible for ensuring that all applicable personnel complete the required training prior to entering the existing jail and for coordinating the addition of personnel throughout the Project.

Completion of CJIS training does not provide unrestricted or unescorted access to the facility. Access shall remain limited to the areas and activities authorized by the Hood County Sheriff's Office.

B. Fingerprinting and Background Screening

Personnel requiring fingerprinting or other background screening shall complete the applicable requirements established by the Hood County Sheriff's Office and its designated CJIS authority prior to receiving the applicable access authorization.

Fingerprinting shall be completed in accordance with the Hood County Sheriff's Office **IdentoGO Fingerprinting Instructions** included with this Exhibit.

The Contractor shall coordinate personnel requiring fingerprinting sufficiently in advance of the date access is required to allow for scheduling, processing, review, and approval.

Completion of fingerprinting or background screening does not independently authorize access to the existing jail or other restricted areas.

C. Security Addendum

Each contractor or subcontractor required by the Hood County Sheriff's Office to complete a Security Addendum shall execute the applicable **FBI Criminal Justice Information Services Security Addendum and Texas Signatory Page**.

Applicable employees shall complete the required employee certification and acknowledgment information included with the Security Addendum.

The Contractor shall coordinate submission of required documentation with the designated Hood County/Sheriff's Office representative prior to the date access is required.

D. Personnel Additions and Removals

The Contractor shall maintain current information regarding personnel requiring access to the existing jail or other secured areas.

The Hood County Sheriff's Office shall be notified prior to any new individual receiving access to the existing jail or other areas requiring prior approval.

The Contractor shall notify the designated Hood County/Sheriff's Office representative within twenty-four (24) hours when an individual with approved access:

- Is removed from the Project;
- Separates from employment; or
- No longer requires access to the facility.

The Contractor shall require its subcontractors to promptly communicate personnel changes so these notification requirements can be maintained.

E. Final CJIS Determination

The Hood County Sheriff's Office designated CJIS authority shall make the final determination regarding CJIS training, fingerprinting, background screening, Security Addendum requirements, and other CJIS-related requirements applicable to specific personnel or work areas.

Personnel shall not be granted the applicable facility access until all required CJIS and access requirements have been completed and authorization has been provided.

5. COORDINATION WITH HOOD COUNTY AND SHERIFF'S OFFICE

Security and access conditions may vary based on the specific work location, jail operations, security conditions, and nature of the Work.

The Contractor shall coordinate questions regarding access, escorts, restricted areas, CJIS requirements, inmate movement, security systems, jail operations, and other facility-security matters through the designated Hood County/Sheriff's Office representative.

The Contractor shall not assume that previous access authorization, unescorted access, or an established work route will remain unchanged throughout the Project. Security requirements and access arrangements may be modified by the Sheriff's Office when necessary to maintain facility security and operations.

The Contractor shall comply with all applicable requirements contained in the attached Sheriff's Office Directive and any authorized updates communicated during the Project.

6. ATTACHMENTS

The following documents are included with and form part of this Exhibit:

Attachment A – Hood County Jail Sheriff's Office Contractor Access, Security & Construction Operations Directive

Attachment B – FBI Criminal Justice Information Services Security Addendum and Texas Signatory Page

Attachment C – Hood County Sheriff's Office IdentoGO Fingerprinting Instructions

HOOD COUNTY JAIL | SHERIFF'S OFFICE

CONTRACTOR ACCESS, SECURITY & CONSTRUCTION OPERATIONS DIRECTIVE

Contractor Expectations and Required Procedures

1. PURPOSE

This directive explains the rules and expectations for contractors, subcontractors, vendors, inspectors, delivery personnel, and other individuals performing work at or within the secure perimeter of the Hood County Jail.

The jail will remain an operating detention facility while construction work is taking place. The purpose of this directive is to make sure everyone understands how construction work will be conducted without compromising the safety and security of inmates, staff, contractors, visitors, or the public.

This directive is not intended to replace the contract, project drawings, project specifications, Texas Commission on Jail Standards (TCJS) requirements, or applicable FBI Criminal Justice Information Services (CJIS) requirements. It establishes the Sheriff's Office's expectations for contractor access and security while work is being performed.

TCJS establishes minimum standards for the construction and operation of Texas county jails and reviews jail construction documents. The current TCJS standards should be followed for the project.

CJIS requirements apply when contractor personnel have access to Criminal Justice Information, CJIS systems, or areas subject to CJIS physical-security requirements. The Sheriff's Office's designated CJIS authority will determine what CJIS requirements apply to a particular person or work area.

2. THE BASIC EXPECTATION

Contractors are welcome on the property to perform authorized work. However, a jail is not a normal construction site. Security and jail operations must always be considered when work is being performed.

- Only authorized people may enter the property or a restricted work area.
- Workers must stay in the area they are authorized to work in.
- Workers may not enter the existing jail simply because they are working on the project.
- Workers may not enter an area that requires an escort without an escort.
- Workers must follow the instructions of Sheriff's Office personnel regarding security and jail operations.
- Contractors remain responsible for their own employees, subcontractors, tools, equipment, materials, housekeeping, and construction work.
- Sheriff's Office personnel are responsible for jail security and operations; they are not responsible for supervising the contractor's workforce or construction activities.

3. TYPES OF ACCESS

For purposes of this project, access will generally fall into three categories.

A. Outside the Secure Perimeter

This is work performed outside the jail's secure perimeter. Approved contractor personnel may normally work without a Sheriff's Office escort as long as they remain in the approved work area and follow the project and facility rules.

B. Inside the Secure Perimeter but Outside the Existing Jail

This is the area most likely to raise questions. A contractor may be allowed to work inside the secure perimeter without a Sheriff's Office employee continuously escorting them when the area has been specifically approved for unescorted contractor work.

Unescorted does not mean unrestricted. Workers must stay in the approved construction area and may not enter the existing jail, inmate areas, restricted areas, or other areas they have not been authorized to enter.

C. Existing Jail and Restricted Areas

The existing operating jail, inmate housing, booking, medical, control, inmate movement areas, and other restricted locations have additional access controls. Workers entering these areas will normally be escorted unless the Sheriff's Office has specifically approved that person's unescorted access.

4. WORK INSIDE THE SECURE PERIMETER BUT OUTSIDE THE EXISTING JAIL

The Sheriff's Office recognizes that the project may require workers to be inside the secure perimeter while construction is occurring outside the existing occupied jail. Continuous escort of every worker in this area is not automatically required.

Workers may be allowed to work without a continuous escort when the Sheriff's Office has approved the area for unescorted contractor access and the following requirements are met:

- The worker has completed all required screening and access procedures.
- The worker has checked in as required.
- The worker stays in the approved construction area.
- The worker uses approved entrances, exits, and routes.
- The worker does not enter the existing jail or another restricted area.
- The construction area is properly separated from the operating jail.
- The worker maintains control of tools, equipment, and materials.
- The worker does not communicate or interact with inmates.
- The worker follows all directions from Sheriff's Office personnel.

The Sheriff's Office may change an access arrangement or require an escort at any time when jail operations, security conditions, the location of the work, or the type of work makes additional control necessary.

5. ESCORTED ACCESS

An escort means an authorized person accompanies the contractor or visitor while the person is in an area where escorted access is required. CJIS guidance defines an escort as authorized personnel accompanying a visitor at all times while in a physically secure location; simply watching someone by camera does not replace an escort.

An escort may be required when a worker:

- Enters inmate housing or an area where inmates are present or may be present.
- Enters booking, medical, control, intake/release, or another restricted area.
- Moves through an area that cannot be separated from inmate or staff movement.
- Works on or near security doors, locks, gates, alarms, cameras, access-control equipment, intercoms, or other security equipment.
- Enters a CJIS area without the authorization required for unescorted access.
- Is a temporary worker or emergency worker who has not been approved for the applicable unescorted access.
- Must move tools or materials through a restricted area.
- Is working during a lockdown, emergency, or other security condition where an escort is required.
- Is directed by the Jail Administrator or designated Sheriff's Office personnel to remain escorted.

6. WHEN SHERIFF'S OFFICE PERSONNEL MAY REQUIRE AN ESCORT

The Jail Administrator, Sheriff's Office security personnel, or another authorized designee may require an escort whenever the escort is necessary to protect jail security, inmates, staff, contractors, the public, Criminal Justice Information, or security systems.

This decision may be based on current conditions. An area that normally allows unescorted contractor access may temporarily require an escort because of inmate movement, a lockdown, an emergency, a security-system issue, staffing conditions, or the specific work being performed.

Contractors should not assume that a Sheriff's Office employee will always be available to provide an escort immediately. Work that requires an escort should be coordinated in advance whenever possible.

7. UNESCORTED ACCESS

Unescorted access must be specifically authorized. It is not automatically granted to every person who has been approved to work on the project.

- Authorization applies only to the person, area, and type of work approved.
- Workers must remain within the approved area.
- Workers must follow all check-in, identification, tool-control, and security requirements.
- Workers may not use another person's badge, key, credential, or access authorization.
- Unescorted access may be suspended or revoked at any time.
- Any worker that is inside this building must be fingerprinted and must have CJIS training.
- Hood County Sheriff’s Office must be notified immediately if any individual is added to or removed from the project within 24 hours.
- Any contractors must sign a security addendum with the Hood County Sherif’s Office for CJIS purposes. All employees who work within the secured security area must sign this addendum.

For CJIS purposes, the Sheriff's Office's designated CJIS authority will determine whether a person needs additional screening, training, background checks, agreements, or other requirements. The FBI explains that personnel-security requirements are tied to access to unencrypted CJI and whether personnel have unescorted access.

8. DAILY ARRIVAL PROCEDURE

Unless the Sheriff's Office has approved a different procedure, contractor personnel shall follow these steps each day:

1. Enter through the designated contractor entrance.
2. Present required identification.
3. Sign in using the jail's required process.
4. Complete any required security screening.
5. Confirm the approved work area.
6. Account for tools and controlled materials as required.
7. Obtain an escort before entering an area where an escort is required.
8. Begin work only after the worker is authorized to enter the work area.

9. DAILY DEPARTURE PROCEDURE

1. Secure the work area.
2. Account for tools, equipment, keys, badges, and controlled materials.
3. Remove or secure loose construction materials and debris.
4. Report missing tools, damage, injuries, security concerns, or other problems.
5. Return controlled access items when required.
6. Sign out before leaving.

10. EMERGENCY ACCESS

The normal access process may not always be practical during an emergency. Emergency access may be allowed when immediate work is needed to protect life, safety, security, essential utilities, or critical jail operations.

- The Sheriff's Office will determine how the worker enters the facility.
- The worker may be required to remain with an escort.
- The worker may be limited to a specific route and work location.
- Tools and equipment may be inspected.
- Emergency access does not create continuing access after the emergency is over.
- Normal screening and access requirements shall be completed afterward when required.
- Emergency work affecting security or life-safety systems shall be coordinated and documented as soon as conditions permit.

12. TOOLS AND EQUIPMENT

The contractor is responsible for the tools and equipment brought onto the property.

- Keep track of all tools entering and leaving secure areas.
- Secure tools whenever they are not being used.
- Never leave tools unattended where inmates could reach them.
- Immediately report a missing tool.
- Keep saws, grinders, drills, cutting tools, torches, pry bars, ladders, cords, and similar equipment under control.
- Secure chemicals, fuels, paints, solvents, adhesives, and other potentially hazardous or security-sensitive materials.
- Provide an inventory when requested.

- Do not assume a Sheriff's Office escort is responsible for the contractor's tools or equipment.

Sheriff's Office personnel may inspect tools, bags, equipment, vehicles, and materials. An inspection does not transfer responsibility for those items to the Sheriff's Office.

13. MATERIALS AND STORAGE

- Store materials only in approved locations.
- Do not block emergency exits, fire lanes, doors, gates, cameras, or security equipment.
- Do not stack materials against the security perimeter.
- Do not place materials or equipment where they could help someone climb, hide, escape, or gain access to a restricted area.
- Secure loose materials at the end of the workday.
- Remove construction debris as directed.
- Materials may be inspected when entering or leaving the secure perimeter.

14. VEHICLES AND DELIVERIES

- Use only approved entrances and delivery routes.
- Park only in approved areas.
- Delivery personnel shall remain in approved areas unless additional access is authorized.
- Large deliveries, cranes, lifts, concrete operations, or equipment affecting the secure perimeter must be coordinated in advance.
- Vehicles may be inspected.
- Do not block emergency vehicle access.

15. DOORS, GATES, KEYS, AND SECURITY SYSTEMS

- Do not prop open security doors or gates.
- Do not bypass, defeat, disable, or interfere with security equipment.
- Do not copy, share, photograph, or keep facility keys or access credentials unless specifically authorized.
- Work affecting locks, doors, gates, alarms, cameras, access control, intercoms, or other security equipment must be coordinated before work begins.
- If a security system must be temporarily taken out of service, the Sheriff's Office must approve the work and the temporary security measures.

16. CJIS AND COMPUTER/SECURITY SYSTEM ACCESS

Not every construction worker is a CJIS user. CJIS requirements depend on what a person can access.

- Do not access CJIS systems or Criminal Justice Information unless specifically authorized.
- Do not connect unauthorized devices to County networks or security systems.
- Do not enter server rooms, communications rooms, security-system rooms, or similar restricted areas without authorization.
- Do not photograph screens, network equipment, security equipment, camera locations, or other protected information without permission.
- The Sheriff's Office's designated CJIS authority will determine which CJIS requirements apply to a worker or work area.

The FBI's current CJIS resources state that physical protection requirements apply to CJI and related systems, and that personnel-security requirements apply to personnel with unescorted access to unencrypted CJI.

17. PHONES, CAMERAS, AND RECORDING

- Do not photograph or record restricted areas without permission.
- Do not use drones, scanning, mapping, or similar equipment in restricted areas without approval.
- Electronic devices may be restricted in certain secure or CJIS areas.
- Do not share jail layouts, security procedures, camera locations, alarm information, inmate information, staff schedules, or other security-sensitive information.

18. WORKING AROUND JAIL OPERATIONS

Construction will occur while the jail is operating. Contractors must expect that jail operations may affect when and how work is performed.

- Do not interfere with inmate movement, meals, recreation, visitation, medical operations, booking/release, emergency response, or other jail functions.
- Control dust, noise, vibration, fumes, odors, water, and other construction impacts.
- Follow directions from jail staff when inmate movement or an emergency requires the work area to be secured or work to stop.
- Work may be delayed or rescheduled because of jail operations or security needs.

19. SHUTDOWNS AND IMPAIRMENTS

Contractors may not independently shut down or disable systems serving the jail.

- Notify the appropriate project and Sheriff's Office representative before a planned shutdown.
- Identify what will be shut down, where it is located, why it is needed, and how long it will be unavailable.
- Identify how jail safety and security will be maintained during the shutdown.
- Obtain approval before starting the shutdown.
- Restore and test the system before returning it to normal operation.
- Immediately report accidental damage or an unplanned outage.

This includes, when applicable, electrical power, water, HVAC, fire alarm, sprinkler, emergency power, locks, access control, cameras, alarms, intercoms, communications, and other critical systems.

20. EMERGENCIES AND LOCKDOWNS

- Stop work when directed.
- Follow Sheriff's Office instructions.
- Do not try to manage a jail emergency.
- Do not enter restricted areas unless directed.
- Do not pursue or interact with inmates.
- Stay clear of emergency responders.
- Report injuries, damage, missing tools, security problems, unauthorized persons, or other concerns immediately.

21. REPORTING REQUIREMENTS

Contractors must immediately notify jail staff of:

- Missing tools or equipment.
- Unauthorized people in the work area.
- Damaged fences, gates, locks, doors, cameras, alarms, or other security equipment.
- Security concerns or suspected security breaches.
- Contraband or suspicious items.
- Injuries.
- Property damage.
- Utility damage or unexpected outages.
- Any situation that could affect the safety or security of the jail.

22. INSPECTIONS

The Sheriff's Office may inspect people, vehicles, toolboxes, bags, equipment, trailers, materials, and other property entering or leaving jail property, consistent with applicable law and facility policy.

Refusal to comply with an applicable inspection may result in denial or loss of access to the facility.

23. AUTHORITY OF THE JAIL ADMINISTRATOR / SHERIFF'S OFFICE

The Jail Administrator, Sheriff, or authorized designee may change, limit, suspend, or revoke contractor access when necessary to protect jail security or maintain normal jail operations.

This may include requiring an escort, changing an approved route, restricting a work area, stopping work, delaying work, or requiring additional security measures.

These decisions may be made based on current conditions. The fact that a worker was previously allowed to enter an area without an escort does not guarantee that the same access arrangement will apply every day.

24. CONTRACTOR RESPONSIBILITY

The contractor remains responsible for its workforce and construction operations even when Sheriff's Office personnel are involved in access or escort activities.

- The contractor supervises its employees and subcontractors.
- The contractor controls its tools and materials.
- The contractor is responsible for construction safety and housekeeping.
- The contractor is responsible for following the approved work plan.
- The contractor must coordinate work that requires Sheriff's Office assistance.
- The contractor must not assume that Sheriff's Office personnel are available to provide continuous escort or construction supervision.

25. ACCESS QUESTIONS — WHO TO CONTACT

The project team shall provide contractors with the name and contact information for the person designated to handle access and security questions.

Questions about access, escorts, restricted areas, inmate movement, security systems, or jail operations should be directed through the designated Sheriff's Office/Jail Administration contact rather than being resolved by individual workers on their own.

26. COMPLIANCE

Training Requirements and Responsibility: The Contractor shall be responsible for identifying, scheduling, coordinating, and providing all training required for its personnel, subcontractors, and suppliers to perform the Work. All training required shall be completed in a timely manner and shall be coordinated so as not to interfere with or delay the Project schedule. Any failure, omission, or delay by the Contractor or its subcontractors in satisfying required training obligations shall be the sole responsibility of the Contractor and shall not constitute a basis for a delay claim, schedule extension, additional compensation, or suspension of the Work. The Contractor shall take all necessary measures to ensure that the Project remains on schedule notwithstanding any such failure.

A violation may result in removal of the individual from the property, suspension or revocation of access, removal of the individual from the project, required corrective action, contract remedies where applicable, or referral for investigation when conduct may violate law.

Nothing in this directive limits the authority of the Sheriff or Jail Administrator to take immediate action necessary to protect the safety and security of the facility.

27. CONCLUSION

The County recognizes that CJIS requirements, security standards, facility policies and operations may evolve throughout the course of the Project. Contractors shall be expected to remain informed of applicable requirements and to reasonably adapt their practices, procedures, and personnel as necessary to maintain compliance with current CJIS standards and County policies.

Requirements shall be communicated in a clear, understandable, and reasonable manner, with consideration given to the Contractor's ability to implement changes without unnecessarily disrupting the progress of the Project. Contractors are expected to approach policy and CJIS updates with an understanding that changes may be necessary to address evolving security requirements, technology, regulatory standards, and operational needs within the correctional facility.

Agency Identification

Agency Name	ORI
HOOD COUNTY SHERIFF'S OFFICE	***TX1110000***
Agency Address: ***400 DEPUTY LARRY MILLER DR***	
City: ***GRANBURY, TEXAS***	Zip: ***76048***
Agency Representative (Title and Name): ***SHERIFF ROGER DEEDS***	
Phone Number: ***817-579-3307***	Fax Number: ***817-408-2797***
Email address	

Contractor Identification

Company Name	Service Providing Agency	
Company Address		
City	State	Zip
Contractor Representative (Title and Name)		
Phone Number	Fax Number	
Email address		

Visit our website www.dps.texas.gov/securityreview for information on submitting vendor/contractor fingerprints.

Email can be sent to: security.committee@dps.texas.gov

Main office number is: (512) 424-5686

Parties may use the following Security Addendum with the Texas Signatory Page or, in their contract, choose to incorporate the Security Addendum by reference. If the Addendum is incorporated by reference into the contract, a copy of the contract must be provided to the TX DPS CJIS Security Office.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM
Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a) (7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

> States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1)under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM
CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Signature of Contractor Employee _____ Date _____

Printed or Typed Contractor Employee Name _____

Sex: ____ Race: _____ DOB: _____ State/ID or DL: _____

Signature of Contractor Representative _____ Date _____

Printed or Typed Name of Contractor Representative _____

Organization Name and Representative's Title _____

Texas Signatory Page

The undersigned parties agree that the *Security Addendum* is now a part of the contract between the entities. The parties agree to abide by all requirements of the *Security Addendum* and the *CJIS Security Policy*, and it shall remain in force for the term of the contract. Any violation of this addendum constitutes a breach of the contract.

To the extent there is a conflict between a confidentiality clause in the underlying contract and the *Security Addendum* and/or the *CJIS Security Policy*, the *Security Addendum* and the *CJIS Security Policy* shall govern any information covered by the *Security Addendum* and/or the *CJIS Security Policy*.

(To be signed and dated by the vendor(s) and law enforcement agency representative(s) who signed the original contract, or at least who have authority to bind each entity – to include subcontractor services; third party service provider if applicable)

ROGER DEEDS
Printed Name of Agency Representative

Signature of Agency Representative — ***SHERIFF OF HOOD COUNTY*** Title

HOOD COUNTY SHERIFF'S OFFICE — ***TX111000***
Agency Name and ORI — Date

Printed Name of Vendor (Contractor) Representative

Signature of Vendor (Contractor) Representative — Title

Vendor Organization Name — Date

Printed Name of Vendor (Sub-Contractor) Representative

Signature of Vendor (Sub-Contractor) Representative — Title

Vendor Organization Name — Date

IdentoGO

Texas Fingerprint Service Code Form

Hood County Sheriff's Office

Service Name: Hood County Sheriff's Office

To schedule your ten-minute fingerprint appointment, simply visit **https://uenroll.identogo.com** and enter the following Service Code

11H32R

Service Code is unique to your hiring/licensing agency. Do not use this code for another purpose.

Criminal History Check Authorization

I certify that all information I provided in relation to this criminal history record check is true and accurate. I authorize the Texas Department of Public Safety (DPS) to access Texas and Federal criminal history record information that pertains to me and disseminate that information to the designated Authorized Agency or Qualified Entity with which I am or am seeking to be employed or to serve as a volunteer, through the DPS Fingerprint-based Applicant Clearinghouse of Texas and as authorized by Texas Government Code Chapter 411 and any other applicable state or federal statute or policy.

I authorize the Texas Department of Public Safety to submit my fingerprints and other application information to the FBI for the purpose of comparing the submitted information to available records in order to identify other information that may be pertinent to the application. I authorize the FBI to disclose potentially pertinent information to the DPS during the processing of this application and for as long hereafter as may be relevant to the activity for which this application is being submitted. I understand that the FBI may also retain my fingerprints and other applicant information in the FBI's permanent collection of fingerprints and related information, where all such data will be subject to comparisons against other submissions received by the FBI and to further disseminations by the FBI as may be authorized under the Privacy Act of 1974 (5 USC 552a). I understand my fingerprints will be searched by and against civil, criminal and latent fingerprints in the Next Generation Identification (NGI) system. I understand I am entitled to obtain a copy of any criminal history record check and challenge the accuracy and completeness of the information before a final determination is made by the Qualified Entity. I also understand the Qualified Entity may deny me access to children, the elderly, or individuals with disabilities until the criminal history record check is completed. If a need arises to challenge the FBI record response, you may contact the agency that submitted the information to the FBI, or you may send a written challenge request to the FBI's Criminal Justice Information Services (CJIS) Division at FBI CJIS Division, Attention: Correspondence Group, 1000 Custer Hollow Road, Clarksburg, WV 26306.

Don't have access to the Internet? You can still schedule an appointment by calling 888.467.2080