CONTRACT, LEASE, AGREEMENT CONTROL FORM

Date:	09/08/2016
Contract/Lease Control #:	C16-2436-COR
Bid #:	NA
Contract/Lease Type:	AGREEMENT
Award To/Lessee:	FLORIDA DEPARTMENT OF LAW ENFORCEMENT
Owner/Lessor:	OKALOOSA COUNTY
Effective Date:	September 8, 2016
Expiration Date:	INDEFINITE
Description of Contract/Lease:	OPERATE/REGULATE CJNET
Department:	COR
Department Monitor:	ROGERS
Monitor's Telephone #:	850-689-5960
Monitor's FAX # or E-mail:	CROGERS@CO.OKALOOSA.FL.US
Closed:	

Cc: Finance Department Contracts & Grants Office

USER NAME PASSWORD LOG IN

Forgot Username? Forgot Password?

Create an Account

Search Results

Current Search Terms: florida* department* OF LAW* enforcement*

Your search for "FLORIDA* DEPARTMENT* OF LAW* ENFORCEMENT*" returned the following results...

Notice: This printed document represents only the first page of your SAM search results. More results may be available. To print your complete search results, you can download the PDF and print it.

Entity **LAW ENFORCEMENT, FLORIDA DEPARTMENT OF**

Status: **Active**

DUNS: 809396781	**CAGE Code: 3C4W8**	View Details
Has Active Exclusion?: No	**DoDAAC:**	
Expiration Date: 08/15/2017	**Delinquent Federal Debt? No**	
Purpose of Registration: All Awards		

Glossary

Search Results

Entity

Exclusion

Search Filters

By Record Status

By Record Type

SAM | **System for Award Management 1.0**

IBM v1.P.50.20160823-0937

WWW4

Note to all Users: This is a Federal Government computer system. Use of this system constitutes consent to monitoring at all times.

CONTRACT # C16-2436-COR
FLORIDA DEPT OF LAW ENFORCEMENT
OPERATE/REGULATE CJNET
EXPIRES: INDEFINITE

CRIMINAL JUSTICE NETWORK (CJNet) USER AGREEMENT

This Agreement, is entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the State of Florida with headquarters at 2331 Phillips Road, Tallahassee, Florida, and the

Okaloosa County Department of Corrections,

with headquarters at
1200 E James Lee Blvd, Crestview, FL 32539,

with the primary ORI of FL046013C, (hereinafter referred to as the User).

Whereas, FDLE is authorized by law to operate and regulate the Florida Criminal Justice Network (hereinafter CJNet) as an intra-agency information and data-sharing network for use by criminal justice agencies located in Florida;

Whereas, the FDLE Director of Criminal Justice Information Services (CJIS) is recognized by the Federal Bureau of Investigation (FBI) as the CJIS Systems Officer (CSO) for the State of Florida, responsible for administering and ensuring statewide compliance with the FBI CJIS Security Policy (CSP);

Whereas, the User requires access to criminal justice information systems provided by FDLE through the CJNet in order to effectively discharge its public duties;

Whereas, FDLE will facilitate the User's requests to participate in the information services provided on CJNet, provided the User agrees to abide by any applicable laws, policies, procedures and regulations related to systems or applications accessed via the CJNet, understanding that FDLE retains full control over the management and operation of CJNet;

Whereas, criminal justice agencies throughout Florida make applications available via the CJNet to Florida's criminal justice community, and the owner of the application controls access to and defines policies for use of the application and information contained therein.

Therefore, in consideration of the mutual benefits to be derived from this Agreement, the FDLE and the User do hereby agree as follows:

SECTION I CJNET FDLE REQUIREMENTS

FDLE is duly authorized and agrees to ensure access to the information services provided on CJNet and adhere to the following:

1. Serve as the CJIS Systems Agency (CSA) for the State of Florida and provide the User with access to criminal justice information as is available through CJNet, and to serve as the means of exchanging criminal justice information between the User and other criminal justice agencies on CJNet.

2. Provide the User with information concerning privacy and security requirements imposed by state policies, laws, rules and regulations. All references herein to policies, operating procedures, operating instructions, operating manuals and technical memoranda with which adherence is required may be found on the CJNet CJIS Resource Center web page.

3. Facilitate access, using CJNet, to other criminal justice information applications or systems that the User may be authorized to use.

4. Determine which purposes qualify as the administration of criminal justice.

SECTION II CJNET USER REQUIREMENTS

By accepting access as set forth above, the User agrees to adhere to the following to ensure continuation of access:

1. USE OF THE SYSTEM: **Use of the CJNet and any system accessed via the CJNet is restricted to the administration of criminal justice or as otherwise specifically authorized or required by statute.** Information obtained from computer interfaces to other systems, by means of access granted through CJNet, can only be used for the administration of criminal justice as defined in 943.045(2) Florida Statutes. It is the responsibility of the User to insure access to CJNet is for authorized purposes only, and to regulate proper use of the network and information at all times. Accessing information and systems provided via CJNet for other than authorized purposes is deemed misuse. The User shall notify the CSO of any sustained/confirmed cases of misuse. In cases of sustained/confirmed misuse, the User shall identify disciplinary actions and the corrective actions taken to prevent future incidents. FDLE reserves the right to deny Criminal Justice Information (CJI) access to individuals who have sustained cases of misuse.

   a. COMPLIANCE: The User shall permit an FDLE appointed inspection team to conduct inquiries with regard to any allegations or potential security violations, as well as compliance and technical policy reviews/audits. FDLE reserves the right to conduct compliance and technical reviews of agencies accessing the CJNet to ensure network security, conformity with state law, and compliance with this user agreement. These compliance and technical reviews are conducted on an as needed basis.

   b. AUDITS: FDLE conducts regularly scheduled compliance and technical security audits of every agency accessing the CJNet to ensure network security, conformity with state law, and compliance with all applicable FDLE, CJNet, regulations and operating procedures. Compliance and technical security audits may be conducted at other than regularly scheduled times.

c. INFORMATION ACCESS: The User will allow only properly screened, authorized personnel performing a criminal justice function to have access to information contained within the CJNet or any criminal justice information system available via the CJNet.

d. WORKSTATION: FDLE is not responsible for the workstation acquisition, maintenance, operation, repair, supplies or workstation operation personnel costs. All costs associated with returning the workstation to operation, other than CJNet maintenance costs, will be the User's responsibility. FDLE will assist with executing trouble-shooting procedures.

e. STANDARDS OF DISCIPLINE: The User shall establish appropriate written standards, which may be incorporated within existing codes of conduct, for disciplining violators of this and any incorporated policy. Violations include but are not limited to accessing CJNet for unauthorized purposes, disclosure of information obtained from CJNet to unauthorized individuals, or violation of CJNet rules, regulations or operating procedures.

2. RELOCATION: Should the User desire to relocate the data circuit(s) and/or equipment connected to CJNet, the User must provide FDLE written notice 90 days in advance of the projected move. All costs associated with the relocation of the equipment and the data circuit(s), including delays in work order dates, will be borne by User unless FDLE has funding to make changes without charge. The repair and cost of any damages resulting from such relocation will be the User's responsibility.

3. LIABILITY: The User understands that the FDLE, its officers, and employees shall not be liable in any claim, demand, action, suit, or proceeding, including, but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the User in entering, removing, or relying upon information transmitted through CJNet.

SECTION III SECURITY REQUIREMENTS

The User agrees to adhere to the following security policies in order to ensure continuation of CJNet access:

1. PERSONNEL BACKGROUND SCREENING: At a minimum, the User shall conduct a state and national fingerprint-based records check on 1) all personnel who are authorized to access state and/or national CJI data or systems, 2) IT personnel who maintain/support information technology components used to

process, transmit or store unencrypted CJI, and 3) other personnel, including but not limited to support personnel, contractors and custodial staff, with unescorted physical or logical access to physically secure locations, as defined in the CSP and/or IT components used to process, transmit or store unencrypted CJI. The User is strongly encouraged to screen the applicant by other available means, e.g., local court records, in addition to the fingerprint-based record check.

a. The User shall submit applicant fingerprints of persons described in Section III, paragraph 1, for positive comparison against the state and national criminal history and for searching of the Hot Files.

b. The results of the fingerprint-based record check shall be reviewed prior to granting access to CJI or components used to process/store CJI, including access for IT support.

1) If a record of any kind exists, the User shall consult the Guidelines for CJIS Access and notify the CSO for review using the CJI Review Request Form found in the CJIS Resource Center web page. Upon notification from the User, the CSO shall review the matter to determine if access is appropriate and officially notify the User in writing of the CSO's decision regarding access.

2) Once the original background screening has been completed, if the User learns that an employee with access to CJI, including any personnel as identified in Section III, paragraph 2, has a criminal history or pending charge(s), the User shall consult the FDLE Guidelines for CJIS Access and notify the CSO. The CSO shall review the facts and circumstances and notify the User in writing regarding access to CJI.

3) The User shall have a written policy for discipline of personnel who 1) access CJNet and/or CJI for purposes that are not authorized, 2) disclose information to unauthorized individuals, or 3) violate CJNet rules, regulations or operating procedures.

c. As the CSA for the State of Florida, the FDLE reserves the right to deny individual user access to any system or related program that is used to process, transmit or store CJI based on valid, articulable concerns for the security and integrity of the information and/or related systems.

d. The User shall ensure the appropriate ORI is used for submission of applicant fingerprints. Fingerprints submitted for positions associated with the administration of criminal justice or as required by the CSP, shall include the User's criminal justice ORI. Fingerprints submitted for any other positions not related to the administration of criminal justice or required by the CSP shall include the appropriate and approved non-criminal justice ORI

2. PHYSICAL SECURITY: The User shall identify facilities, areas, rooms, etc. where CJI is accessed, processed and/or stored to determine physical security requirements as identified in the CSP. The User may designate a facility, area, room, etc., either a physically secure location or a secured area, as defined in the CSP, provided the appropriate requirements are met. Access shall be limited to persons needing access for completion of required duties. The User shall have a written policy that ensures and implements security measures, secures devices that access CJNet and prevents unauthorized use or viewing of information on these devices. The use of password protected screen blanking software is recommended for devices that access CJNet when the operator may leave the computer unsupervised. FDLE reserves the right to object to equipment location, security measures, qualifications and number of personnel who will be accessing CJNet and to suspend or withhold service until such matters are corrected to FDLE's reasonable satisfaction.

3. ADMINISTRATIVE SECURITY: The User shall designate individual agency contacts, as described below, to assist the User and FDLE in ensuring compliance with this Agreement. Training for these positions is provided by FDLE, and the User shall ensure that its designee is keenly aware of the duties and responsibilities of each of the following positions. FDLE reserves the right to object to the User's appointment of a LASO and FALCON AAA based on valid, articulable concerns for the security and integrity of CJNet or related programs/systems. The User shall provide FDLE with up-to-date contact information for these positions.

   a. LOCAL AGENCY SECURITY OFFICER: The User shall designate a Local Agency Security Officer (LASO) to ensure compliance with the CSP. Within six months of assignment to the position, the LASO is encouraged to complete an approved LASO training made available by FDLE.

   b. In addition to the LASO, there are other points of contact and positions necessary to manage applications and facilitate communication between the User and FDLE. These positions are identified on the Agency CJIS Contact Form, which may be found on the CJNet CJIS Resource Center website under CJIS Forms and Publications.

4. MANAGEMENT CONTROL AGREEMENTS: In situations where data processing/information services, law enforcement dispatch functions or human resources functions are provided by a non-criminal justice governmental entity, the User shall enter into a management control agreement as required by the CSP. In situations where governmental structure or hierarchy does not support or permit an agreement between the parties involved, a directive which includes all of the provisions for a management control agreement identified in the CSP may be substituted.

5. INTERAGENCY AGREEMENTS: The User shall execute an Interagency Agreement with any other criminal justice agency to which criminal justice information services are outsourced, including but not limited to information

technology related functions. The User shall consult with FDLE to determine if a given function requires an Interagency Agreement.

6. TECHNICAL SECURITY

   a. The User shall maintain, in current status, and provide upon request by FDLE a complete topological drawing, which depicts the User's network configuration as connected to CJNet. As required by the CSP, this documentation shall clearly indicate all network connections, service agencies and interfaces to other information systems. The User shall provide FDLE with a list of all User satellite offices or subunits that access the CJNet or available CJNet applications via the User's CJNet connection.

   b. The User shall ensure all devices with connectivity to CJNet employ virus protection, anti-spam and anti-spyware software and such software shall be maintained in accordance with the software vendor's published updates.

   c. The User shall ensure all devices and/or networks with connectivity to both the CJNet and the Internet are protected by a firewall solution, as specified in the FBI CJIS Security Policy.

   c. CJI, including but not limited to information obtained from the CJNet, may only be accessed via computers or interface devices owned by the User or by the contracted entity. Vendors under contract with the User to perform the administration of criminal justice may be allowed to use their own devices for access provided all requirements of the FBI CJIS Security Addendum are satisfied and member CJIS Online Security Awareness Training is current.

   d. The User shall ensure that CJNet-only devices have a Windows or network type password to prevent unauthorized access.

   e. To ensure appropriate security precautions are in place, and upon approval from the FDLE Network Administration staff, the User may employ wireless network connectivity (for example the 802.11 wireless networking protocol).

7. SECURITY TRAINING: The User is responsible for complying with training requirements established in CSP and the rules, regulations, and policies established by FDLE and other CJNet applications. The User is responsible for remaining current in the applications, procedures, and policies and ensuring personnel attend these training sessions.

   a. All User personnel who access CJI for the administration of criminal justice shall complete CJIS Online Security Awareness Training, including but not limited to criminal justice officials, e.g., Police Chiefs, Sheriffs, Judges, State Attorneys, etc.

   b. The User shall maintain training records for all personnel with access to CJI, i.e., CJIS Online Security Awareness Training.

c. The User shall require all IT personnel, including any vendor, responsible for maintaining/supporting any IT component used to process, store or transmit any unencrypted CJI, to successfully complete and maintain in current status the CJIS Online Security Awareness Training provided by FDLE.

8. COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY: The User shall have a written policy documenting the actions to be taken in response to a possible computer security incident. The policy shall include identifying, reporting, investigating and recovery from computer security incidents. The User shall immediately notify the CSO of any suspected compromise of the CJNet.

9. SECURITY AUTHORITY: All policies, procedures and operating instructions contained in the CSP, FDLE CJIS/Informational/Technical Memoranda, and operating manuals, are hereby incorporated into and made a part of this agreement, except to the extent that they are inconsistent herewith or legally superseded by higher authority.

10. PRIVATE VENDORS: Private vendors which, under contract with the User, are permitted access to information systems that process CJI, shall abide by all aspects of the FBI CJIS Security Addendum.

a. The contract between the User and the vendor shall incorporate the FBI CJIS Security Addendum to ensure adequate security of CJI.

b. The User shall ensure all vendor employees are appropriately screened prior to granting the vendor employees access to CJI. Vendor employee fingerprints submitted by the User to FDLE as required by the CSP shall be .taken/rolled/printed by a recognized law enforcement agency or an FDLE approved third party vendor. NOTE: A vendor may not fingerprint its own employees.

c. The User shall maintain the Security Addendum Certification form for each member of the vendor staff with access to information systems that processes CJI.

d. The User shall ensure all vendor employees with access to CJI have received the appropriate security awareness training via the CJIS Online Security Awareness Training application and are in current status.

e. The User shall ensure private vendors permitted such access are aware of the provisions of Section 817.5681, F.S. regarding breach of security of personal information.

f. The User shall contact FDLE for review prior to entering into a contract or agreement with a private vendor in the course of which state or national CJI is processed, stored or transferred from the User's physically secure location to a vendor owned or operated facility(s) (e.g., cloud services.)

g. The User shall maintain and keep current a list of all vendor employees who have been authorized access to CJI.

11. USERNAMES and PASSWORDS/AUTHENTICATION: The User shall ensure that all personnel, including IT support and vendors, have a separate and distinct username and password/ authentication for the software/interface used to access CJI.

    a. Individual users shall refrain from sharing passwords and/or other authenticators, including but not limited to smart cards, tokens, public key infrastructure (PKI) certificates, etc., used to access CJI or CJNet related systems.

    b. Individual users shall refrain from using another individual's account or session for the purpose of accessing CJI or other CJNet applications.

    c. Individual users shall refrain from caching credentials/passwords for access to systems/applications used to process or store CJI.

    d. All personnel with access to any system or application that processes or stores CJI for maintenance or administration purposes shall be uniquely identified.

12. INDIVIDUAL USER ACCESS: The User shall deactivate individual user access to all CJNet applications and other state/federal systems containing CJI, including but not limited to FBI Law Enforcement On-line (LEO), upon separation, reassignment or termination of duties, provided individual user access is no longer required for the administration of criminal justice.

13. OFF SITE STORAGE/PROCESSING OF CJI: The User shall contact and receive approval from the CSO prior to entering into an agreement with a noncriminal justice governmental agency for off-site storage or processing of CJI (often referred to as cloud computing or cloud services.)

14. ACCESS CONTROL: In situations where CJNet access is provided to the User's offices or subunits via the User's network, the User will ensure proper controls are in place and maintained to restrict access to criminal justice personnel assigned to permanent duty locations within the state of Florida.

SECTION IV MISCELLANEOUS REQUIREMENTS

1. PENALTIES AND LIABILITIES: Any non-compliance with the terms of this Agreement concerning the use and dissemination of criminal history information may subject the User's officers or employees to a fine not to exceed $11,000 as provided for in the Code of Federal Regulations, Title 28, Section 20.25, and/or discontinuance of service. Moreover, certain offenses against system security and

the information contained therein are crimes under Florida Statutes and can result in criminal prosecution.

2. PROVISIONS INCORPORATED: The User shall be bound by applicable state laws, regulations and the rules of FDLE to the same extent that the User would be if such provisions were fully set out herein. Moreover, this Agreement incorporates both present and future law, regulations and rules.

3. TERMINATION: Either party may terminate this Agreement, with or without cause, upon providing advanced written notice of 45 days. Termination for cause includes, but is not limited to, any change in the law that affects either party's ability to substantially perform as originally provided in this Agreement. Should the aforementioned circumstances arise, either party may terminate or modify the Agreement accordingly.

   a. FDLE reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating this Agreement or any pertinent federal or state law, regulation or rule.

4. MODIFICATIONS: Modifications to the provisions in this Agreement shall be valid only through execution of a formal written amendment.

5. ACCOUNTABILITY: To the extent provided by the laws of Florida, and without waiving any defenses or immunities to which the User may be entitled, the User agrees to be responsible for the negligent acts or omissions of its personnel arising out of or involving any information contained in, received from, entered into or through CJNet.

6. ACKNOWLEDGEMENT: The User hereby acknowledges the duties and responsibilities as set out in this Agreement. The User acknowledges that these duties and responsibilities have been developed and approved by FDLE to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the CJNet. The User further acknowledges that failure to comply with these duties and responsibilities will subject its access to various sanctions as approved by FDLE. These sanctions may include termination of CJNet services to the User agency. The User may appeal these sanctions through the CSA.

7. TERM OF AGREEMENT: This agreement will remain in force until it is determined by FDLE that a new agreement is required. The User should initiate the execution of a new agreement when a change of agency chief executive or official occurs.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF USER AGENCY Okaloosa County Department of Corrections

USER CHIEF EXECUTIVE or OFFICIAL

Stefan W. Vaughn **TITLE** Chief
(PLEASE PRINT)

Stefan W. Vaughn
(SIGNATURE)

DATE May 25, 2016

WITNESS Christina Rogers **TITLE** Office Supervisor

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY **Charles I. Schaeffer** **TITLE** **Director**
(PLEASE PRINT)

(SIGNATURE)

DATE 6/13/16

WITNESS **TITLE** Admin Assistant

Zan Fedorak
Purchasing Manager
Zan Fedorak 9/8/16