Louisiana State Police Centralized Vendor Vetting Program (CVVP) FAQ

WHAT IS THE CVVP?

The Louisiana State Police (LSP) provides a vast array of services that either directly or indirectly support the exchange of Criminal Justice Information (CJI) to other Criminal Justice Agencies (CJA) and Non-Criminal Justice Agencies (NCJA). As the CJIS Systems Agency (CSA) of Louisiana, LSP has a requirement to manage and audit all CJA's and NCJA's with direct and indirect access to CJI.

CJA's that utilize vendors for the administration of criminal justice functions are responsible for ensuring their vendor meets the CJIS Security Policy (CJISSECPOL) requirements and that all personnel have undergone vetting requirements. To ease the burden on CJAs and their vendors, the LSP established and maintains the Centralized Vendor Vetting Program (CVVP) as a single source for Louisiana CJAs to fulfill initial vendor compliance requirements identified within the CJIS Security Policy (CJISSECPOL).

HOW DOES THIS AFFECT MY AGENCY?

If your vendor does not complete the CVVP, it will be a non-compliant finding on your audit and it will be your responsibility to ensure the vendor is properly vetted by your agency. If your vendor completes the CVVP, your agency will not need to be solely responsible for CJIS vetting your vendors. Your agency would still be required for ensuring the vendor completes the process, maintains compliance, and assists in escalation procedures when the vendor becomes unresponsive or non-compliant.

HOW DOES THIS BENEFIT MY COMPANY?

The CVVP was designed to ease the burdens of vendors meet the CJISSECPOL requirements. Upon successful completion of the CVVP, your vendor would be listed on the LSP website with an approval status. Your personnel would also be vetted on the state level easing the financial burden on your company. Rather than completing training, security addendum and fingerprinting requirements for each CJA you support, personnel would only need to complete items once with the CVVP. Please note that while the LSP provides a centralized vendor vetting process to help meet requirements, any CJA you work with can still elect to complete separate vetting or additional personnel vetting requirements outside of the CVVP.

HOW DOES A VENDOR GET ENROLLED IN THE CVVP?

The CVVP is only open to vendors who are working with Louisiana CJA's. To ensure this requirement is met, each vendor must be "sponsored" by a CJA they work with. To start the process, vendors must execute a sponsorship form with a CJA they work with and a vendor agreement. The required forms can be found at https://www.lsp.org/forms/ under LSP CJIS Centralized Vendor Vetting Program. Completed forms must be submitted to lsp.vendorvetting@la.gov.

WHO SHOULD BE OUR VENDOR ADMINISTRATOR?

The Vendor Administrator will be the liaison between your vendor and the LSP CVVP Team for ensuring all Phase 1 and Phase 2 items are completed and any other matters concerning the use and misuse of CJIS systems. This individual will be contacted for due dates, follow ups, and escalations. If there are additional team

members you would like to include during Phase 1 or Phase 2 to help facilitate items, that is acceptable.

Additional duties of the Vendor Administrator include but are not limited to:

1. Ensuring all Vendor personnel who support the CJI contract are enrolled and have completed CJIS Online Security Awareness Training and the LA Cybersecurity Awareness Training (recertified annually)
2. Ensuring all Vendor personnel who support the CJI contract have submitted a Criminal History Record Review Form and have completed a fingerprint based background check
3. Uploading each of Vendor personnel's signed/completed CJIS Security Addendum Certification Page into each individuals' CJIS Online record
4. Notifying LSP of any employment changes to Vendor personnel who support the CJI contract, during the course of any engagement with a Criminal Justice Agency
5. Notifying LSP of any Vendor Administrator or Vendor changes including name, contact information, or address and submit a Vendor Change Form
6. Immediately notifying LSP if any approved Vendor support personnel are arrested for any offense, criminal or civil
7. Responding to audits and requests for compliance related information in a timely manner, including the annual compliance check-in questionnaire, and the triennial audit.
8. Validating, annually, that assigned Vendor personnel continue to support the CJI contract in Louisiana

WHAT SHOULD I EXPECT FROM THIS PROCESS?

The CVVP team will review form submissions and approve a vendor proceeding in the process. The CVVP process is separated into two phases. In Phase 1, you will first be assigned an abbreviated pre-audit questionnaire within CJIS Audit to gather background information such as the solutions/products being offered, whether any subcontractors are utilized, if you are a CJIS Vendor or a Non-CJIS Vendor, and to determine your eligibility for the CVVP.

If it is determined that you are a Non-CJIS Vendor, you will only complete the initial pre-audit questionnaire and then proceed to Phase 2 of the CVVP. If you have a SOC II/Type 2 attestation or are authorized with FEDRAMP moderate or higher, you will be required to submit your attestation and CJIS policies as a pre-audit artifact. Upon review, if you have a SOC2/Type II (and/or bridge letters) or are authorized with FEDRAMP moderate or higher with no concerning findings that would be non-compliant with CJISSECPOL and your Information Security Policy specifically states your company adheres to all requirements in the CJISSECPOL, you will not need to complete the full vendor audit.

If you are a CJIS Vendor and do not have a SOC II/Type 2 attestation or do not have FEDRAMP moderate or higher authorization, a full vendor audit will be assigned to you after the pre-audit questionnaire is completed. The technical audit includes questions related to personnel security, media protection, physical security, network security, access control, incident response, auditing and accountability, and systems and information integrity. If

determined in the pre-audit questionnaire that you provide more than one solution/offering that has the potential to access CJI data, you shall complete a vendor audit for each solution/offering.

Upon successful completion of Phase 1, an approval package consisting of the Vendor Sponsorship form, the Vendor Agreement, a copy of the audit(s), and a recommendation by the CVVP team will be forwarded to the LSP Review Committee for approval. If the LSP Review Committee determines vendor denial, the Vendor Administrator will receive an official Phase 1 denial letter detailing the denial. If the LSP Review Committee determines approval, the Vendor Administrator will receive an official Phase 1 approval and will be provided Phase 2 instructions.

Phase 2 of the CVVP consists of personnel vetting and approval. The following requirements will need to be completed per individual supporting the CJI system or having indirect access to CJI. The CVVP team will set your company up within CJIS Online if you do not currently have a vendor account.

1. Having all personnel identified within CJIS Online
2. Having all personnel complete:
    a. A Criminal History Review Request Form- *Required every five years*
    b. A state and national fingerprint-based record check- *Required every five years*
    c. CJIS Security Awareness Training- *Required annually and within CJIS Online*
    d. Louisiana Cyber Security Training- *Required annually*
    e. A Security Addendum Certificate Page- *CJIS Vendors Only*

A vendor is not completely vetted until receiving Phase 2 Personnel Approval letters.

WHAT IF A SUBCONTRACTOR SUPPORTS OUR SOLUTION/OFFERING?

All subcontractors that support your solution/offering must be identified in the Vendor Agreement and during the initial pre-audit questionnaire. If the identified subcontractor's work enables access to CJI data, they will be required to complete the CVVP. You will not receive Phase 1 Approval until all identified CJIS subcontractors have received Phase 1 Approval.

WHAT TIMELINES DO I HAVE TO MEET?

You will have 15 calendar days to submit Pre-Audit responses and/or artifacts and 30 calendar days to submit responses and/or artifacts for the full vendor IT audit. If additional responses are required, you will receive 15 additional calendar days. In Phase 2, you will receive 15 calendar days to have all personnel complete vetting requirements.

WHAT IF I CAN'T MEET A TIMEFRAME?

The CVVP team will send reminders to your Vendor Administrator on items that are due. If you cannot meet a due date provided to you, be proactive and let us know estimated timeframes and the reasons for the delay. If you become unresponsive or timelines are not met without communication, the CVVP team will begin escalation procedures. If you enter escalation, your sponsoring agency will be notified and your access to CJI may become revoked.

The LSP may remove a Vendor from the program for non-compliance with the LSP CJIS Vendor Agreement. In this situation, TBS shall produce a denial letter to be provided to the Vendor Administrator to advise them of the redress procedures and timeframes.

Vendors who request to be on a hold for any reason will receive a three month due date to resume the process. If this timeframe is not met, the LSP reserves the right to remove the vendor from the process and will provide formal notification to the vendor administrator and sponsoring agency. If a Vendor removes themself from the CVVP, the Vendor Administrator must notify the LSP and provide the reasoning for removal.

Should the vendor wish to restart the process, submission of a new vendor agreement and sponsorship form will be required. In addition, all components of the CVVP process will need to be completed regardless of previous submissions.

WHAT IF OUR PERSONNEL ALREADY COMPLETED A BACKGROUND CHECK?

In order to make the fingerprint status available to all CJA's in Louisiana and be vetted on the state level, personnel will be required to complete a new fingerprint-based background check through the CVVP. All personnel are also subjected to a fingerprint based background check every five years to remain in compliance.

DO ALL EMPLOYEES WORKING FOR A CJIS VENDOR NEED TO UNDERGO A FINGERPRINT-BASED BACKGROUND CHECK?

No. A CJIS vendor may have other facets of their business which are separate from their CJIS business. However, all vendor employees with responsibilities for configuring systems and networks with direct access to CJI, as well as employees with physical and/or logical access to CJI must also undergo a fingerprint-based background check. This may include the same type of support personnel as are fingerprinted within the law enforcement agency including human resources staff, janitorial staff, and others.

WHY WAS MY EMPLOYEE DENIED FROM THE CVVP?

The CJIS Security Policy governs the Louisiana State Police's decision-making process when evaluating vendor employees for access to CJI and participation in the Vendor Management Program. Section 5.12.1.2.4-5 of the policy states that:

"A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be

disqualified. [...] Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants."

If a felony conviction and/or outstanding arrest warrant is discovered for a Vendor Management Program applicant, the Vendor Administrator will be notified that the applicant is not authorized to participate in the program and shall not have physical, logical, or situational access to criminal justice data. Under CJIS Security Policy section 5.12.1.2.3, the denial of access can be appealed to the LSP.

If **any** criminal record is found and a final disposition is not present, the LSP will deny the individual CJI access and the applicant will be declared ineligible for the program.

Please note: while an applicant may qualify for the Vendor Management Program, individual criminal justice agencies reserve the right to conduct further background investigations into contracted personnel and impose more stringent criteria for accessing their facilities and/or data.

CAN EMPLOYEES STILL GET FINGERPRINTED IF WE ARE NOT LOUISIANA BASED?

Yes. Upon entering Phase 2 and having personnel submit the required Criminal History Review Request Form, fingerprinting instructions will be provided that includes an option to complete digital fingerprinting or hard copy submission via Mail through IdentoGo. Hard copy submissions will **not** be accepted if they are mailed to LSP.

WHAT IS THE VENDOR ADMINISTRATOR RESPONSIBLE FOR AFTER APPROVAL?

Vendor and Personnel Changes

The Vendor Administrator shall notify the LSP by email (LSP.VendorVetting@la.gov and cjis-iso@la.gov) within 24 hours that an approved vendor employee has left the organization or been reassigned to duties no longer supporting the CJI related contract. At the same time, if the employee has left the organization, the vendor administrator shall mark the employee inactive in CJIS Online. If an employee is added to the Vendors personnel list, the Vendor Administrator shall notify the LSP by email and complete CVVP personnel vetting of the new staff prior to the employee receiving access to CJI.

The Vendor shall notify the LSP by email (LSP.VendorVetting@la.gov and cjis-iso@la.gov) within five (5) business days that the Vendor Administrator has changed and a Vendor Change Form must be submitted.

In the event the Vendor intends to withdraw from the LA CVVP, the Vendor Administrator shall notify LSP.VendorVetting@la.gov and cjis-iso@la.gov. As stipulated in the CJIS Security Addendum, the LSP has the right to conduct an audit to ensure proper disposal of CJI. If the Vendor no longer contracts with the Sponsoring Agency from initial vetting, the Sponsoring Agency shall notify LSP.VendorVetting@la.gov and cjis-iso@la.gov.

Arrest Notifications

In the event the Vendor, the Vendor Administrator, or any vendor personnel are made aware that a Vendor employee approved to support a CJI contract has been arrested or convicted, the Vendor Administrator shall notify the LSP within 24 hours by email. The notification shall include:

- ❑ Subject line "Vendor Personnel Arrest Notification"
- ❑ Vendor company name
- ❑ List all Louisiana criminal justice agencies contracted
- ❑ Name of subject who has been arrested
- ❑ New Criminal History Record Request Form

The notice shall be sent to LSP.VendorVetting@la.gov and cjis-iso@la.gov to trigger a new background check for that staff member. Personnel may be subject to further personnel vetting upon notifications. All personnel are subjected to a fingerprint based background check every five years to remain in compliance.

HOW DO I MAINTAIN MY APPROVAL STATUS?

Upon approval of both Phase 1 and Phase 2 in the CVVP, you will be added to an annual cycle. One year from the month you receive Phase 2 approval, you will be sent a compliance check-in questionnaire. This questionnaire will include the results of the previous audits completed and a list of approved personnel. Your vendor administrator will be required to provide responses within 15 calendar days to validate any technical or personnel changes. If the technical configuration of your services and/or products have changed, you will be required to complete Phase 1 again. If there were any personnel additions or removals, the CVVP team will provide further instruction as to what is needed. Any new additions will be required to complete all requirements from Phase 2 of the process.

Every approved vendor will be required to complete Phase 1 of the process again every three years, regardless of configuration changes, from their last audit whether from initial vetting or through a compliance check in.

Example 1: No Technical Changes
Year 1: Initial Approval
Year 2: Annual Check In with no technical changes
Year 3: Annual Check In with no technical changes
Year 4: Triennial Vendor Audit

Example 2: Identified Technical Changes
Year 1: Initial Approval
Year 2: Annual Check In with technical changes and full vendor audit
Year 3: Annual Check In with no technical changes
Year 4: Annual Check In with no technical changes
Year 5: Triennial Vendor Audit

WHAT IF I AM NON-COMPLIANT AFTER INITIAL APPROVAL?

If during an additional audit it is determined you are not compliant, you will receive a Plan of Action and Milestones (POAM) form outlining non-compliant findings. Your vendor administrator will be required to execute the POAM form and provide corrective action plans and dates the CVVP team will review and approve. The CVVP team will follow up with you every six (6) months or based on approved timeframes, whichever is sooner. If approved timeframes are not met, you will be required to submit a new POAM form. If you are found to be non-compliant again during your next audit, whether due to further technical changes identified in the annual check in or when recompleting Phase 1 again, you will be removed from the approval list and your access to CJI will be terminated.

WHAT IF WE ENCOUNTER A SECURITY INCIDENT?

If your company encounters any type of security incident, you must report it immediately, but not to exceed one hour, after discovery to the CJIS Systems Officer (CSO) and CJIS Information Security Officer (ISO) by submitting a Security Incident Reporting Form to lsp.vendorvetting@la.gov. The form can be found at https://lsp.org/media/yc1psx32/lsp-security-incident-reporting-form.pdf. Upon notification, your access may terminated and/or you may be removed as an approved vendor upon an internal investigation. Further instructions will be provided after this internal investigation outlining what requirements must be met to reinstate access and/or receive CVVP approval as needed.

WHAT DOCUMENTS WILL I NEED TO SUBMIT DURING MY AUDIT?

If you are a Non-CJIS Vendor, you will be required to submit a list of company employees that will need to be vetted.

If you are a CJIS Vendor with a SOCII/Type II Attestation and/or have FEDRAMP authorization (moderate or higher), you may be required to provide the following information to complete your audit(s):

1. A list of company employees that will need to be vetted
2. Your SOCII/Type 2 Attestation and/or any bridge letters or your FEDRAMP authorization (moderate or higher)
3. A copy of your company's Information Security Awareness and Training Policy
4. A copy of your company's Systems and Information Integrity Policy
5. A copy of your company's Identification and Authentication Policy
6. A copy of your company's User Account- Access Validation Policy
7. A copy of your company's Local Security Policy
8. A copy of your company's Media Protection policy
9. A copy of your company's Physical Protection policy
10. A copy of your company's Disciplinary policy
11. A copy of your company's Incident Response policy
12. A copy of your company's Personally Identifiable Information policy
13. A copy of your company’s network diagram

If you are a CJIS Vendor without a SOCII/Type II Attestation or FEDRAMP authorization (moderate or higher), you may be required to provide the following information to complete your audit(s):

1. All artifacts listed above
2. Interface Control Document or Workflow Diagrams for any developed applications
3. Anti-Virus Policy
4. Asset Management Policy
5. Lost/Stolen Device Policy
6. Lost/Stolen Media Policy
7. Data Loss Prevention Policy
8. Data Handling Policy
9. Business Continuity Plan
10. Software Development Life Cycle (SDLC)
11. Peer Code Review Policy
12. Any security assessment performed in the last 24 months (internal or external assessments included)

Note: The CVVP team may request additional documentation from your company during the audit.