



This document is to be completed for new or upgraded technology acquisitions, contracts, and projects. Please submit with all other proposals and agreement terms for review by the County Information Security Officer according to directives in Administrative Memorandum B-1. All questions must be answered fully.

Submitting Department _____

Submitter's Name Corey Kennedy

Phone _____

Section 1: Vendor Information

Name: Gemalto Cogent Inc.

Corporate Phone #: 626-325-9600

Address: 639 N. Rosemead Blvd

City: Pasadena

State: CA

ZIP: 91107

Technical Support Contact Methods:
(Select all that apply)

☒ Phone: 866-500-2347

☐ IM/Chat

☒ Email:

☒ Web Portal

SalesForce

Technical Support Coverage Hours:

☒ 24x7x365

☐ Business Hours M-F 8-5 Pacific

☐ Other

24x7

Does the vendor provide a dedicated account manager or representative for escalating problems or incidents?
If yes, please provide name.

☒ Yes ☐ No

Gordon.He@gemalto.com

Does the vendor maintain any formal security policies & procedures to comply with industry requirements?

☒ Yes ☐ No

How often is the vendor's security posture reviewed?

System Design and Delivery

Will the vendor provide a copy of their last security audit?

☒ Yes ☐ No

Does the vendor have any third-party certifications or attestations, such as FedRamp, FIPS 140-2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, TRUSTe or SOC 1/SOC 2/SSAE 16/ISAE 3402? If yes, provide certification or attestations.

☒ Yes ☐ No

Yes - when solution requires it - FIPS 140-2 ANSI, NIST, CJS. More available upon request

Section 2: Product Information

Product Name: CAFIS

No. of Users: 25-30

Does the product have technical constraints to the number of concurrent users it can support?

☐ Yes ☒ No

☒ This is an upgrade or renewal for existing technology currently in use in the County

Location:

☒ On-Premise

☐ Hosted (Cloud/Off-site)

☐ Hybrid (On-Premise/Cloud)

Product Description and Purpose: Please include information that will identify the function, business process, and the departments/divisions who will use it.

The Automated Fingerprint Identification System (AFIS) stores and compares fingerprint data from Ilvescan bookings in the jail. The AFIS is used by the County identification personnel to positively ID-subjects in custody and in the field.

Mobile AFIS readers which our deputies will be outfitted with, will allow them to establish the true identity of individuals while in the field. Mobile AFIS readers (Blue Check) will only transfer fingerprints to the deputy's Mobile Digital Computer (MDC) to which it is paired. The SO does not anticipate implementing this feature for the next 6 - 12 months, until after the core CAFIS system (which has reached End-Of-Life) has been implemented.

Integration: Does the product integrate or interface with any other existing or planned products or services used either at the County, or with another third-party County vendor? This would include requirements for integration or use of the County's email System, ServiceNow, or other systems.

☒ Yes ☐ No

California DOJ for Livescan TOT transmission and/or Latent Gateway searches to DOJ or FBI.

Has the application been subjected to any breaches? If yes, include separately, enacted steps to mitigate including response and escalation processes.

☐ Yes ☒ No

none known

Known Vulnerabilities?

☐ Yes ☒ No

none known

For details on Data Sensitivity and Data Criticality, please see the Section 6 References of this document

Data Sensitivity: ☐ Public ☐ Internal ☒ Confidential ☐ Restricted

Data Criticality: ☐ Useful ☒ Important ☐ Essential

Section 3: Administrative Controls

Configuration and System Hardening: Does the product offer a baseline configuration or system hardening tool that can protect the product against confidential data disclosure or service disruption? **Please provide system configuration diagram

☒ Yes ☐ No

Released Code is validated by vulnerability scanners

Backup and Restore: Does the product offer features to backup and restore user data, configurations, and application code?

☒ Yes ☐ No

In addition to RAID configuration, a external HDD (physically attached to the server in the secured Data Center) is included for backup and recovery.

Does the product integrate with CommVault Storage Services and API (the County's backup platform)?

☒ Yes ☐ No

If there is a backup process performed by Vendor: ☒ Yes ☐ No

How often: When Changes are made on the system

Retention period: At least 4 years

Encrypted? ☐ Yes ☒ No

When stored? County Data Center

Data at Termination of Agreement: Will the data be returned? ☒ Yes ☐ No

What assurance is provided for complete removal?

typically the county retains HDDs, We can perform DOD Wipe if requested

Section 4: Security Controls

Monitoring and Event Management: Describe how the product can be monitored for performance, reliability, and security. Include how the product reacts to events that are raised during normal operations.

Zabbix (open-source), SVRMON (Cogent in-house)

Can the product forward events to a central log repository or System Event and Incident Management (SEIM) platform

☐ Yes ☒ No

Patching: Describe how the product is patched and updated. Include how frequently the vendor provides security fixes and updates.

Product vulnerability patching is included, OS patching is on as needed basis by vendor. TSU can also apply patches while working with vendor.

If the hardware is onsite, can County engineers apply patches

☒ Yes ☐ No

If hosted, please provide version, service pack, patches, and how will the server be maintained to the latest patch level?

NA

Anti-Virus Protection: Is anti-virus running?

☒ Yes ☐ No

Will the product be affected by servers or endpoints that run anti-virus/anti-malware protection? If yes, provide details on what exclusions are required for the product to work effectively.

☒ Yes ☐ No

SO will run County-standard Anti-Virus software and work with Gemalto and ISD to establish a workable whitelist. The SO recognizes the importance of good/effective backup and recovery strategy and will work with Gemalto and ISD to establish a

Employees: Have employees undergone a background check process?

☒ Yes ☐ No

Will the provider use a subcontractor or 3rd party service provider?

☐ Yes ☒ No

If yes, please attach and provide for each subcontractor, the security and privacy agreement.

If yes, provide security and privacy agreement for each subcontractor.

SaaS: Is the product 100% web-based?

☐ Yes ☒ No

What are the browser security configuration requirements?

Please describe browser security configuration requirements.

Is the portal ADA compliant with Section 508 of the Rehabilitation Act and follows the principles of responsive web design?

☐ Yes ☐ No

Disaster Recovery: Is the location of the server, if hosted, in an area prone to natural disaster?

☐ Yes ☒ No

County Facility or Data Center

Is there a disaster recovery plan in place?

☐ Yes ☐ No

Identity and Authentication Management:

Does the product provide for, or support *identity an authentication integration with via other credentialing systems or protocols?*

Note: SAML is the preferred choice for integration with San Mateo County systems

☒ Yes ☐ No

If yes,
please specify

☐ SAML
☐ OAuth
☐ MFA

☒ Active Directory
☐ LDAP
☒ Other

If other, please indicate.

Password Management:

How are accounts provisioned and managed (include deprovisioning and removal)?

AD, User Group Manager (UGM) and Single Sign-On (SSO)

Does the product provide for password management that meets the County password policy for complexity, expiration, reuse, and lockout? *See Section 6 References for more information about San Mateo County's Password Policy*

☒ Yes ☐ No

1. All users have a single account with unique account ID?
2. First time password must be unique and changed upon initial login?
3. Password must be changed every 60 days?
4. Password must have at least 8 characters and 1 character from *three* of the following: lowercase, uppercase, number, special character?

☒ Yes ☐ No

☒ Yes ☐ No

☒ Yes ☐ No

☒ Yes ☐ No

Does the product provide for password self-reset capability?

☒ Yes ☐ No

How are passwords stored?

Encrypted?

☒ Yes ☐ No

Access Management: Does the product allow for privileges to be assigned to both individuals and 'groups' of individuals in order to support the use of 'Roles' for access permissions? Please describe method used.

☒ Yes ☐ No

User Group Manager (UGM) and Single Sign-On (SSO)

Encryption: Identify and describe whether the product encrypts data during different states—i.e., at rest, in use, and in transit. Also include credentials (usernames, passwords, etc.)

Data-in-transit

No, locally-housed in a protected private network. SO intends to work

Data-in-use

No, locally-housed in a protected private network

Data-at-rest

No, locally-housed in a protected private network

Credentials

AD encryption

Auditing: Does the product provide a mechanism for auditing system activity and/or reporting of that activity? Examples of auditing include user login/logout, user actions, data export, and permission changes.

☒ Yes ☐ No

User actions are logged in database

Section 5: Cloud/Hosted Services

Data Sovereignty: Does the vendor keep all the data within the United States? Please provide location(s) where San Mateo County's data will be stored.

this is a non cloud solution - Data resides with County

Tenancy: Describe how San Mateo County data resides with other customer data in the hosted environment—i.e., is the data co-mingled in a single database, or are there separate customer databases?

Please enter details here.

Hosted Platform: Please describe the vendor's technology platform in the hosted environment—both application, database, and/or other layers (e.g., Ruby on Rails, Redis Cache, MongoDB)

Please describe platform here.

Third Party Services: Does the vendor use any third-party services (e.g., for development, QA, helpdesk, integration services, offsite backup locations, etc.) where the third-party vendors have access to San Mateo County data?

☐ Yes ☒ No

Please provide additional detail including names of vendors.

Network Defenses: Please describe how the vendor's network perimeter is protected, including whether an IPS/IDS and anti-virus system is activated, and if there is a central logging facility for perimeter events

SO's 10.50 subnet-based Firewall

Service Levels and Incident Response:

What is the service level for this hosted product, and how does the vendor guarantee that level for its customers? Include how the vendor notifies customers of incidents that do not meet service levels.

Cogent SOP document

Data Loss Events: Has the vendor experienced any data loss incidents which required reporting to regulatory authorities in the past 24 months?

☐ Yes ☒ No

If yes, please provide additional details.

Forensic Analysis: Who would perform a forensic analysis of a breach if one were to occur at the vendor site?

☐ Yes ☐ No

NA

IP Restrictions: Does the vendor's hosted site have the capability to restrict access to San Mateo County's public IP address space?

☐ Yes ☐ No

NA

Section 6: References

Password Policy

The County of San Mateo's Information Security Policy requires new technology implementations that use passwords to adhere to the following password requirements:

County of San Mateo Password Requirements

1. All users must have unique account IDs that identifies a single account owner
2. First time password must be unique to an individual, and require change upon initial login
3. The permanent / long term password requires an enforceable change every 60 days
4. The password must enforce a minimum of at least 8 characters, and contain at least one character from *three* of the following:
 - a. Lower Case
 - b. Upper Case
 - c. Numbers
 - d. Special Characters

Data Classification Standards

In order to apply the proper security safeguards to digital assets, the County of San Mateo classifies new technology both to a Sensitivity and Criticality class. The following information defines those classification standards and is added as a resource to answering the questions in Section 2, 'Product Information'.

Sensitivity Class	Description	Criticality Class	Description
Public	Public data is information assets that can be disclosed without restrictions. Permission to release or share data does not require approval. Examples: <ul style="list-style-type: none">• Information typically included on the San Mateo County website - County addresses, department phone numbers, generic department emails.• Applications, request forms, press releases.	Useful	Useful data is information assets helpful to the mission of the health system, but whose availability isn't necessary to maintain day-day operations. Useful data is often characterized with low risk in case of loss or compromise. Examples: <ul style="list-style-type: none">• Printers and fax machines where there are multiple alternatives• Images of workstations that can be rebuilt if necessary• Training materials• Reports that can be reproduced from original sources
Internal	Internal data is intended to be used only within San Mateo County, but disclosure poses minimal business impact, and may even be subject to release per the County's Open Data Policy. Permission to share publicly is to be given by the data steward or through committee approval. Examples: <ul style="list-style-type: none">• Business plans, budgets, vendor lists, vendor contracts.• Memo's, meeting minutes, policies/procedures	Important	Important data is information assets whose availability is valuable for maintaining day-day operations, but service levels can tolerate an unscheduled period of downtime. Downtime for Important data is acceptable at certain days/hours in given week, but usually no longer than three (3) consecutive days for any single event. Examples: <ul style="list-style-type: none">• Software systems that are only used during the weekday and/or normal business hours• Software systems where data sets updates are not updated frequently, and business tasks can be deferred without service impact• Managed Services ran by the State of California• Systems where contingency plans can maintain service levels
Confidential	Confidential data is information assets that, if compromised, could adversely impact customers or San Mateo County business. This information is to receive data protection for storage and transport, should only be used for business purposes, and where possible be identified as confidential by those who use it. Examples: <ul style="list-style-type: none">• Social Security Numbers, Driver's license number, credit cards• Personal addresses, phone numbers, private email addresses• Access codes or passwords A compromise of Confidential data is to be reported as a security incident, as outlined in the County's Incident Response Plan.	Essential	Essential data requires nearly continuous uptime. Business processes are adversely affected with even a small amount of unscheduled downtime, impacting the job performance of the workforce and services to customers. Access to these information assets typically requires 24x7 availability, and must be rigorously protected. Examples: <ul style="list-style-type: none">• EMR systems• Identity Management Applications• Core networking equipment
Restricted	Restricted data is Confidential data—except, the business impact for compromise is much greater. This includes civil penalties, regulatory redaction for organizational credentials, and formal notification to federal, state, and local authorities. Restricted data typically involves information that has contractual, legal, or regulatory obligations to protect the data in the utmost manner. Examples: <ul style="list-style-type: none">• Medical Records and other Protected Health Information (PHI)• Employee criminal background checks The organization as a whole—along with data stewards—is responsible for designating data as Restricted. A compromise of Restricted data is to be reported as a security incident, as outlined in the County's Incident Response Plan, and included notification to the County's Privacy Officer.		

Section 7: Non-Compliance

Please explain area(s) of non-compliance. Provide information as to the services or systems that would be impacted as well as the proposed remediation/mitigation, if any.

NOTE: All non-compliance must file an Information Security Risk Acceptance Form

See completed form.

Section 8: Other Documents

Please include any pertinent documents, diagrams of network, and/or data flow architecture

Documents included? ☐ Yes ☐ No

Information Security Risk Acceptance Form

Instructions: Fill out all portions of the form applicable. If you require more space, please attach your responses to this form. Once finished, please send this form to the Information Security Officer – ISD – Stormy Maddux.

Vendor Name: Gemalto Cogent Inc.

Departmental Contact Information:

Name and title of Originator: Gloria Kanu - IT Director, SMC Sheriff's Office

Email and Phone Number of Originator: gkanu@smcgov.org

Policy/Standard/Guideline you are requesting an exception from:

Name the policy, standard, or guideline that is impacted by this request.

Non-Standard Hardware - Use of HP physical Server. This is a vendor-supported system and vendor will do the OS-patching as they are currently performing. Virtualization will be added in the next upgrade as we are performing a like-for-like upgrade at the moment due to time constraint by first upgrading the core system and then adding other features and functionality at a later date.

Specialized implementation of County Antivirus and use of non-standard backup system to augment CommVault Backup since an external hard

Summary of the request:

Describe the policy, standard, guideline, or admin memo that is impacted by this request.

We will not be in compliance with the County Hardware/Antivirus/Backup Policies, specifically the use of non-standard hardware for our Cogent Upgrade. Antivirus whitelist will be developed and non-standard backup system will be used to augment CommVault.

Overview of the service/system impacted:

Describe the department, user name, host name, application, or service that is impacted by this request.

Sheriffs Office -

No PII travels between mobile "blue-check" device and the client – only fingerprints. Even then, that connection is through a secured connection, MDCs in the patrol car.

Risk Classification:

LOW



MEDIUM



HIGH



Does the application/service for which the security exception applies store, process, transmit, or use any of the following types of data in any way?

	Yes	No
Social security numbers	✓	
Driver's license numbers or state identification numbers (for CA or any state)	✓	

Visa or passport numbers or related data	✓
County employee records	
Credit or debit card numbers	
Credit card transaction approval data	
Personal health information (whether included in medical records or otherwise)	
Banking account or other financial account numbers and/or access codes or passwords for the County of San Mateo or any other person or entity	
Computer user names and/or passwords	✓
Personal contact data for County workforce, business partners, or members of the public	

If you answered "yes" to any of the above items, please provide a brief explanation of how the data is used in the application/service:

These items are used for identification purposes.

Benefits of accepting this risk:

We will be able to upgrade an otherwise out-of-date system.

Describe the impact to the system/project/users if the risk is not accepted:

Delays to the upgrade project which will jeopardize the SO's ability to conduct ID functions .

With regards to the Antivirus implementation, vendor can either supply an Anti-Virus client or provide the list of folders to whitelist. The reason given by the vendor is that there are folders with very high IO, and this can impact search/response times. Alternatively, SO can change expectations on system performance.

Describe mitigating controls in place:

Describe the technical and procedural controls that will be implemented to address the vulnerabilities and risks above. How are you going to minimize or mitigate the risks this solution causes?

Vendor will continue to maintain the system - no actual vulnerabilities.

SO will run Anti-Virus software and work with Gemalto and ISD to establish a workable whitelist

~~The CAFIS servers and designated workstations are connected to the CAL ID Network. The recommendation from Gemalto is not to introduce~~

After controls what is the remaining risk and what is the risk level:

Describe the type and magnitude of remaining vulnerabilities and risks after the controls have been implemented.

None

Risk Acceptance Request:

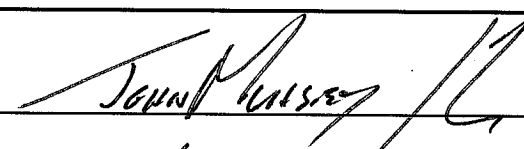
I understand that compliance with County policies and standards is expected for all workforce members, departments, organizational units, information systems, and communication systems. The service, application or business owner is seeking a risk acceptance decision for the following deployment.

I accept responsibility for the risk associated or created by the exception described above. I also understand that this exception is temporary and will work to implement the plan to ensure compliance in the future.

Signed by: Gloria Kanu, Service or Business Owner

Department: Sheriffs Office

Signature Date: rg
gkanu@smcgov.org Digitally signed by gkanu@smcgov.org
DN: cn=gkanu@smcgov.org
Date: 2019.01.25 14:45:29 -0800

Signed by: , Department/Agency Head

Signature Date: 2/7/19

Signed by: _____, Information Security Officer

Signature Date: _____

Date of Next Review: _____ (AT LEAST ANNUAL)

Appendix A

Criticality Matrix

	Most Critical <i>Highest level of sensitivity</i>	Critical <i>Moderate level of sensitivity</i>	Least Critical <i>Very low, but still requiring some protection</i>
Legal Requirements	Protection of data is required by law (e.g., HIPAA and Criminal Justice data elements and other personal identifying information protected by law)	The institution has a contractual obligation to protect the data	
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information that provides access to resources, physical or virtual	Smaller subsets of Most Critical data from a department	
Data Examples	<ul style="list-style-type: none"> • Medical • Criminal Justice • Prospective employee • Personnel • Financial • Contracts • Physical plant detail • Credit card numbers • Certain management information • Personally identifiable information 	<ul style="list-style-type: none"> • Information resources with access to Most Critical data • Financial transactions that do not include Most Critical data (e.g., telephone billing) • Unidentifiable small subsets of Most Critical data 	<ul style="list-style-type: none"> • Personal directory data (e.g., contact information) • E-mail • Institutionally published public data