|  |  |  |
| --- | --- | --- |
|  |  |  |



**Volume I**

**Case Management Platform Requirements**

Table of Contents

[1. General Characteristics 3](#_Toc482626938)

[2. Service Capabilities for the PPS-CM platform solution 3](#_Toc482626939)

[3. Technical Capabilities for the PPS-CM platform solution 3](#_Toc482626940)

[3.1 Hosting Environments 4](#_Toc482626941)

[3.2 Key Performance Parameters and Maintainability 5](#_Toc482626942)

[3.3 Measures of Effectiveness 6](#_Toc482626943)

[3.4 User Provisioning 7](#_Toc482626944)

[3.5 Single Sign On 8](#_Toc482626945)

[3.6 Interfaces 8](#_Toc482626946)

[3.7 Security and Privacy 9](#_Toc482626947)

[4. Technical Support and Maintenance 9](#_Toc482626948)

[4.1 Maintenance Support 9](#_Toc482626949)

[4.2 Training Strategy 9](#_Toc482626950)

[Exhibit A: PPS-CM Internal and External Interfaces 10](#_Toc482626951)

# 1. General Characteristics

The solution shall have the following general characteristics:

1. A purpose-built platform solution with an underlying data base configuration/structure that supports multiple subjects connected to a single client/case.
2. FedRAMP accredited security and an established access control system.
3. Ability to support geographically (CONUS and US territories) distributed users.
4. Audit tracking of data access and modifications (transactions).
5. Ability to store and access a widely diverse set of digital assets (multimedia and documents).
6. A logical User Interface that is intuitive, transparent, and will allow data capture from a number of sources.
7. Web enabled access to allow rapid storage and retrieval from a variety of mobile devices.
8. An automated notification mechanism that informs officers when their records have been accessed and by whom.
9. A platform solution that is scalable, offers a basis for future features and capabilities, and is highly accessible.

# 2. Service Capabilities for the PPS-CM platform solution[[1]](#footnote-1)

The contractor shall meet the detailed requirements specified in Volume III - PPS-CM Business and Technical Matrix: ‘Platform – SRM’ tab.

# 3. Technical Capabilities for the PPS-CM platform solution[[2]](#footnote-2)

The contractor shall meet the detailed requirements specified in Volume III - PPS-CM Business and Technical Matrix: ‘Platform – TRM’ tab. The following high-level technical capability areas list the PPS requirements for the PPS-CM platform solution:

1. Application Architecture Components
2. Virtualization and Hosting Architecture
3. Virtualization and Hosting Architecture
4. Standards and Portability
5. Developer Tools
6. Programmable APIs
7. Marketplace of third party add-ons
8. Content Delivery Network (CDN)
9. DevOps-Code Deployment and Life Cycle management
10. Logging, Monitoring and Alerting
11. Web Front-end and Networking
12. Scaling and High Availability
13. IT Service Management (ITSM)
14. Compliance, security and access control
15. Platform Governance
16. Support and Service Levels
17. SSO Platform
18. Data/Content Platform
19. Business Intelligence / analytics platform
20. Data Access Platform
21. Data Access Components
22. Business Entity Components
23. Synchronous and Asynchronous Business Logics
24. Workflow
25. Custom Assemblies
26. COTS plug-Ins
27. Common/Shared Web Services
28. Reporting Tool
29. User Access Channel
30. Infrastructure Services
31. Application Integration

## 3.1 Hosting Environments

The contractor will provide a hybrid cloud solution where the data is hosted on-premises and the platform is hosted off-premise. The PPS-CM shall include access to a pool of Virtual Machines (VMs) that can be used for the systems development lifecycle processes.

The contractor’s GovCloud shall provide Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The hosted GovCloud environments shall include systems management, monitoring, security auditing, and 24/7 operations support as is provided for all other infrastructure resources required for PPS-CM platform solution.

The solution must be in GovCloud for application platform (Off-premises) and AOUSC On-promises cloud hosting center for content via Hybrid Cloud approach.

The contractor shall provide the infrastructure to all of the development teams supporting the PACTS Modernization program. Developer VMs can be ordered in several sizes suitable for uses that range from web servers to large database server/hosts, each with a choice of operating systems. The Government has identified requirements for at least nine (9) types of system environments to support the PACTS Modernization program as shown in Table 1.

|  |  |
| --- | --- |
| Environment | Purpose |
| Development (DEV) | Development environment (separate environments for major components of the PPS-CM platform solution) |
| Development Integration (INT) | Integration and test environment |
| System Test (TST) | Formal system testing to validate integration and interoperability among all components |
| Performance Test (PERF) | Performance testing (load, capacity, response time) |
| User Acceptance Test (UAT) | User acceptance testing prior to deployment at IOC |
| Training (TRN) | User training and related documentation (ongoing) |
| Staging (STG) | Validation of deployment configuration prior to transition to production |
| Production (PROD) | Production environment |
| Disaster Recovery (DR) | Disaster recovery environment |

Table 1: PACTS Modernization Project Hosting Environment

## 3.2 Key Performance Parameters and Maintainability

Key performance parameters (KPPs) are specified for the PPS-CM platform solution in Table 2 below. These are the overall objectives for the PPS-CM platform solution, and the contractor shall meet the performance requirements.

The availability KPP in Table 2 shall drive the PPS-CM platform solution maintainability requirements in terms of mean time to restore service (average time to restore service after a failure), mean downtime (time that the PPS-CM platform solution is not operational due to service incident or preventive maintenance including logistic and administrative delays), and planned downtime (time that the PPS-CM platform solution is not operational due to corrective and preventive maintenance including logistic and administrative delay time).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | KPP | Threshold | Objective | Comments |
| 1 | Response Time: Transaction response time refers to the time required for completion of an individual transaction.  Specifically, the time it takes from a workstation request to a workstation response, which is tested at the end user device level. Test time begins when the user hits enter after filling out the appropriate transaction criteria and ends when the intent of the transaction is accomplished, for example when search results appear on the results page.  Response time for search includes responses from all data sources queried. | The system shall provide operationally acceptable transaction response time\* for individual transactions across the system, not to exceed 5 seconds 95% of the time. | The system shall provide a transaction response time\* for individual transactions across the system, not to exceed 3 seconds 99% of the time. | \*Response time excludes transaction processing time on systems external to the investigative case management application.  (For example, processing within the PPS-CM application must not add more than 5 seconds to the time required for an external database to process a request with regard to Threshold or 3 seconds with regard to Objective.) Response time is calculated only for devices directly connected to An AOUSC network and does not include remote devices (i.e., connected through VPN, mobile device running over wireless network, etc.). |
| 2 | Concurrent Users:  The system shall be able to handle a high level of users, measured by the number of concurrent users accessing the system at the same time. | No less than 1,000 users accessing the system at the same time with system capability allowing all users to conduct business transactions concurrently within the application. | No less than 7,000 users accessing the system at the same time with system capability allowing all users to conduct business transactions concurrently within the application. | Approximately 90% of system transactions are database reads. Database updates consists of the remaining 10%. |
| 3 | Availability:  The PPS-CM platform solution shall achieve the required level of Operational Availability (Ao). | Ao > 99.07% | Ao > 99.97% | Required level of monthly Operational Availability for the PPS-CM platform solution components. |

Table 2: KPPs for the PPS-CM platform solution

## 3.3 Measures of Effectiveness

The following measures of effectiveness (MOEs) describe high-level capabilities pertaining to PPS-CM platform solution capability objectives the contractor shall meet:

* Ability for all users with appropriate access to view cases and all associated documents, subject records, and links within five seconds of being created when they are accessing the system from a device directly connected to an AOUSC DCN network
* Ability for users to create a client record and have that record available for posting to PPS-CM platform solution within five seconds (via an PPS-developed data service)
* Ability for users to perform all work flow related to cases, case documents, and subject records (i.e., opening/creating, approving, modifying, deleting)
* Ability for users to link cases to case documents and subject records/lookouts
* Ability for users to link client record to case documents
* Ability of the PPS-CM platform solution to receive and present search responses from all sources with which the system interfaces within five seconds of the source data being made available to the PPS-CM platform solution
* Ability of the PPS-CM platform solution to generate audit trails to facilitate reconstruction of events on demand
* Reduced data entry time via elimination of duplicative requests for input of data from users
* Ability of the PPS-CM platform solution to interface with internal PPS/AO systems and external systems as described in other sections of this SOW.

## 3.4 User Provisioning

New agents shall need to be provisioned to the PPS Active Directory (AD) prior to being provisioned in the PPS-CM platform solution. This process is outside the scope of the PPS-CM platform solution user provisioning process. Once users are added to PPS AD, the process to provision a user to the PPS-CM platform solution can be initiated by a local District staff admin according to the three-step process shown in Figure 3. The process for updating user profiles follows these same steps. The steps are explained in more detail below.



Figure 3: PPS-CM User Provisioning for the PPS-CM platform solution

Step 1: The DSA will create a user profile in the PPS-CM platform solution as follows:

* The DSA will enter user-name, middle-name, last name in a screen in the PPS-CM platform solution application
* The PPS-CM platform solution application will query PPS AD to retrieve user(s) matching this query
* The DSA will browse the list (if more than one is returned) and manually make a determination of which one of the users is most likely the individual he/she is intending to provision in the PPS-CM platform solution
* The DSA will then select that user from the list
* This completes the user-create process (some information from AD will be pre-populated in the screen).

Step 2: The DSA will then: a) define role(s) for this agent and b) assign an office code to this agent (this office code is based on an existing legacy office hierarchy).

Step 3: The DSA will then a) assign a supervisor to this user (filtered list of users based on the office selected) and b) assign a DSA user to this agent.

The PPS-CM platform solution shall develop a static office hierarchy of its own and host it in the PPS-CM platform solution database; therefore, a user’s office information will not be retrieved from the PPS AD. Users will need to self- register upon initial logon to the PPS-CM platform solution. The PPS-CM platform solution shall present these users with a screen to update their personal information including their AOUSC email addresses.

The SSO process will use the PPS AD for initial user authentication. The PPS-CM platform solution shall then validate the user to the PPS-CM platform solution if that user has been provisioned in the PPS-CM platform solution user. Though all the PPS-CM platform solution users have an active PPS AD, not all PPS AD users have access to the PPS-CM platform solution. Merely having an active PPS AD, does not in and of itself mean a user can perform functions in the PPS-CM platform solution.

## 3.5 Single Sign On

The PPS-CM platform solution shall implement standards-based mechanisms, such as Security Assertion Markup Language (SAML 3.0), to achieve SSO within the AOUSC and CMSO infrastructure. Authentication will be externalized to the PPS-CM platform solution. JENIE is currently used as a proxy to SSO for Active Directory authentication of individual users. The PPS-CM platform solution shall implement industry standard Web Access Management (WAM) methods to enable SSO for application components of the PPS-CM platform solution.

## 3.6 Interfaces[[3]](#footnote-3)

The PPS-CM platform solution shall query and search specified data sources that are internal to PPS or AOUSC and external to AOUSC. Information shall be requested from interface partners by calling Simple Object Access Protocol (SOAP)-based web services exposed via the PPS Interface Hub which will be implemented by the PPS Interfaces Team. In addition, the PPS-CM platform solution shall interface directly with the PPS DSS and Judiciary Enterprise Data Warehouse. The PPS-CM platform solution shall authenticate and authorize individual users accessing interface services, and shall include the user’s authenticated identity in each call for auditing purposes. The PPS-CM platform solution shall authenticate to the PPS Interface Hub using digital certificates and shall use secure socket layer (SSL) encrypted channels when transmitting or retrieving sensitive information via an interface. The PPS-CM platform solution shall process inbound interface information such as training and certification updates and asynchronous request notifications. Table 7 in Exhibit A summarizes the interface operations that shall be supported by the PPS-CM platform solution.

## 3.7 Security and Privacy

The system shall be compliant with all relevant security controls outlined in the Federal Information Processing Standard (FIPS), the Federal Information Security Management Act (FISMA) and Federal RAMP to include, but not limited to, the ability of the federal government to perform a security certification and accreditation process to obtain an authorization to operate that will be signed by the federal principal without delay to system deployment. The system shall be FedRAMP High compliant.

# 4. Technical Support and Maintenance

## 4.1 Maintenance Support

The contractor shall provide maintenance support of the PPS-CM platform solution. This includes the bug fixes/patches, routine maintenance and upkeep of the PPS-CM platform solution licenses and upgrades on any supplied products associated with the PPS-CM solution, and upgrade frequency for the installed PPS-CM platform solution.

## 4.2 Training Strategy

The contractor shall provide existing training plans and materials, user guides, operations manuals, and maintenance manuals for their PPS-CM platform solution and shall provide these training-related items to the Government. The contractor shall provide subject matter expertise regarding the proposed solution, its function, and corresponding training/user readiness lessons learned to support the Government in developing the training program for the PPS-CM platform solution.

# Exhibit A: PPS-CM Internal and External Interfaces

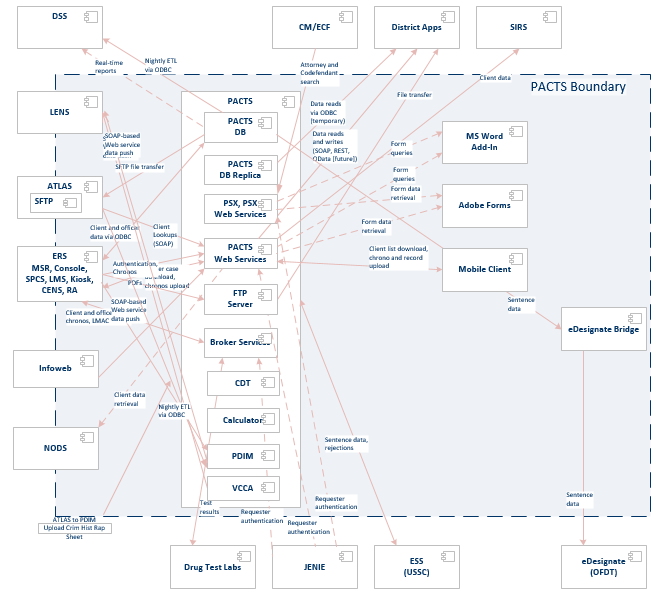


Figure 7: PACTS System Interfaces

Table 7: Key PACTS System Interfaces Description

|  |  |  |  |
| --- | --- | --- | --- |
| Interface Title | Description | Direction | End Point |
| **ATLAS** | The Access to LAw enforcement Systems (ATLAS) is a web-based application that allows users to access information from two law-enforcement computer systems which contain criminal history information. | Web Service Outbound  (one way) | NCIS |
| PACER | The Public Access to Court Electronic Records (PACER) is an electronic public access service that allows users to obtain case and docket information from federal appellate, district, and bankruptcy courts. | JDBC | CM/ECF |
| BOP By Name | Search for federal inmates by name incarcerated from 1982 to present using the Federal Bureau of Prisons (BOP) Inmate Locator tool. | Pull  (one way) | Sentry |
| BOP By FBI Number | Search for federal inmates by FBI Number incarcerated from 1982 to present using the Federal Bureau of Prisons (BOP) Inmate Locator tool. | Pull  (one way) | Sentry |
| BOP By Register Number | Search for federal inmates by Register Number incarcerated from 1982 to present using the Federal Bureau of Prisons (BOP) Inmate Locator tool. | Pull  (one way) | Sentry |
| BOP Offender Release Report | Bureau of Prisons Offender Release Report. | Pull  (one way) | Sentry |
| National Offender /Defendant Search by Name, SSN | National Offender/Defendant Search by Name. | Web Service  (one way) | PACTS |
| ERS Enroll Client | The Electronic Reporting System (ERS) allow the judiciary to exchange case-related information with defendants, offenders, and treatment providers using kiosks, the Internet and phones. | JDBC | PACTS |
| ERS Assign Questions Sets | The Electronic Reporting System (ERS) allow the judiciary to exchange case-related information with defendants, offenders, and treatment providers using kiosks, the Internet and phones. | JDBC | PACTS |
| ERS Report By Client | The Electronic Reporting System (ERS) allow the judiciary to exchange case-related information with defendants, offenders, and treatment providers using kiosks, the Internet and phones. | JDBC | PACTS |
| ERS Client Assignment by Officer | The Electronic Reporting System (ERS) allow the judiciary to exchange case-related information with defendants, offenders, and treatment providers using kiosks, the Internet and phones. | JDBC | PACTS |
| Victim Notification System | National Victim of Crime Notification System. |  |  |
| OPERA | Offender Payment Enhanced Report Access (OPERA) is an application within the DSS project. It uses data from district instances of Civil and Criminal Accounting Manager, and so does not make any PACTS connections. |  | DSS |
| **LENS** | The Law Enforcement Officer Notification system that allows probation and pretrial services officers to electronically notify local law enforcement agencies of changes to the case history of offenders under supervision as required by the Violent Crimes and Criminal Act of (VCCA) 1994. | Push  (one way) | PACTS |
| **SIRS** | The Safety and Information Reporting System (SIRS) is used to manage data related to the dangerous or potentially dangerous incidents officers face in working with defendants and offenders; collect and track information about offender searches pursuant to special court-ordered search conditions and the evidence and property seized or abandoned; and manage and track training programs on the district and national level. The AO uses SIRS data to develop and enhance training programs to increase officer safety. | Web Service (DLL) | PACTS |
| **Risk Assessment** | Risk Assessment tools. Access to ERS Risk Assessment products is provided from PACTS via a link to Risk Assessment in the Portal to External Resources navigation menu. PACTS passes authentication information for the user to the Risk Assessment application so that a second log-in is not necessary. As with the rest of ERS, a combination of calls to Broker Services and direct JDBC connections to retrieve and push data is used. | ESB and JDBC | PACTS |

1. See Separate attachment: Volume III - PPS-CM Business and Technical Matrix: Platform - SRM [↑](#footnote-ref-1)
2. See Separate attachment: Volume III - PPS-CM Business and Technical Matrix: Platform - TRM [↑](#footnote-ref-2)
3. See Exhibit A: PPS-CM Internal and External Interfaces [↑](#footnote-ref-3)