

HIJIS SERVICE SPECIFICATIONS

Services are being solicited for the Hawaii Criminal Justice Data Center (HCJDC) to assist with new development and enhancements, testing, and implementation of tasks related to incident reporting query in the Hawaii Integrated Justice Information Sharing (HIJIS) system.

OVERVIEW

The HIJIS program is a significant directive as it aims to provide criminal justice and non-criminal justice agencies the ability to share information across the whole of the justice and public safety enterprise, facilitate information exchange with key agencies, and to leverage national information sharing standards and best practices.

Partnering agencies to the HIJIS program span over to State and Federal agencies and the four counties, Maui County, Honolulu County, Hawaii County and Kauai County.

HIJIS ARCHITECTURE

HIJIS is a collection of technology services, built on a distributed architecture, that automates flows of information among Hawaii justice partners. HIJIS implements national information sharing standards (such as GRA, GFIPM and NIEM) and favors use of open-source over proprietary solutions. The core HIJIS functionality is built on the Java platform and exposes functionality through a variety of SOAP and REST web services as well as a user-facing secure web portal. HIJIS enables secure single sign-on and federated identity management through the use of the SAML 2.0 standard which also ensures secure and controlled access to HIJIS services.

Key components:

- HIJIS broker – a centralized collection of intermediary services that mediate communications between justice systems. These services are responsible for routing, transforming, validating, logging and securing messages that flow through the HIJIS environment.
- HIJIS adapter – transforms interactions that conform to the services standards (SOAP, REST, etc.) into interactions that conform to the providing system. Adapters receive messages from a service in accordance with the service specifications and “adapts” the message to the service provider environment.

The HIJIS architecture and core services enable:

1. Federated Query– allowing authorized users to search for records (criminal history, warrants, firearm registrations, etc.) across disparate criminal justice business systems.
2. Subscription/Notification (Rap Back) – notifying criminal justice and non-criminal justice stakeholders if individuals of interest (employees, supervision subjects, etc.) have criminal history involvements nationwide.
3. Workflow automation – automating system-to-system work flows as required by the criminal justice process, such as routing information between law enforcement, prosecution and courts.

4. Activity Logging – tracking of activity across the HIJIS platform to support audit requirements and usage metrics.
5. Program administration – tools that allow HCJDC staff to administer the HIJIS program.

TIME PERIOD FOR SERVICES

The required services for assistance with the HIJIS system will be needed between November 2020 through June 2021. Extension of services will be evaluated at the end of the method of agreement.

SCOPE OF SERVICES

The contractor will provide development and support services for the specified HIJIS Program initiatives and related applications. This includes administrative support, design, development, testing and implementation. The HCJDC requires that the scope of services utilizes the existing HIJIS architecture.

Incident Reporting Query

This initiative is to provide incident reporting information from each of the four county police departments through a single query request via the HIJIS. Incident reports are a collection of arrest and non-arrest information in each of the counties records management system (RMS). The four counties are Honolulu, Maui, Hawaii and Kauai.

This solicitation is to complete the incident reporting initiative for Maui Police Department (MPD) and Kauai Police Department (KPD).

The following is to be provided by the offeror:

1. Identify the incident reporting information exchange requirements, create an IEPD and develop service specifications for the incident reporting query.
2. Development and technical assistance for the MPD and KPD RMS interfaces to HIJIS.
3. Modify other HIJIS components to complete this exchange including the broker and HIJIS portal application.
4. Perform end-to-end testing and validate that incident reporting functions as specified by the HCJDC.
5. Troubleshoot emerging issues as specified by the HCJDC.
6. Implement the incident reporting query for MPD and KPD.
7. Provide technical documentation of the components added or modified to implement this initiative.
8. Work with HCJDC staff for hands-on training and knowledge transfer.

EXPERIENCE

It is highly desirable that the Contractor have significant prior experience in policy and planning, justice standards, security, systems analysis, application software, communication tools, operating systems, networking services, data management, systems administration, and customer support. It is recommended that the Contractor have knowledge and experience in the following areas:

1. Global Justice Reference Architecture (JRA)

2. National Information Exchange Model (NIEM)
3. Service Oriented Architecture (SOA)
4. Java, JavaScript, JSP, Enterprise Java Beans, Java Business Integration Standards
5. J2EE, J2SE, Java ServerFaces (JSF)
6. AJAX, HTML, XHTML, CSS
7. Document Object Model (DOM)
8. XML
9. XSLT
10. XMLHttpRequest object
11. Universal Message Service
12. .NET Framework
13. C#
14. Structured Query Language (SQL)
15. PHP, PERL
16. Oracle Developer
17. Domino/Notes
18. Simple Object Access Protocol (SOAP)
19. ESB connector containers, service interface intermediaries, service containers, and appropriate adapters
20. Policy and planning services (e.g. privacy impact assessment, privacy policy development, data standards, infrastructure planning and management, project auditing, etc.)
21. Security protocols (e.g. Kerberos, PPTP, IPsec, SSL, SSH, GFIPM, Extensible Access Control Markup Language (XACML), etc.)
22. Encryption standards (e.g. DES3, PGP, WPA2, etc.)
23. Security services (e.g. intrusion prevention, secure messaging, wireless security, firewax, system security management, directory services, network access control, federated identity, etc.)
24. Secure content management (e.g. LDAP, SAML, active directory, authentication, authorization, integrity, confidentiality, non-repudiation and reliable delivery, WS-ReliableMessaging standards, database persistence of messages in transit for failure recovery, JRA Web Services Service Integration Profile (WS-SIP), Message Transmission Optimization, Mechanism(MTOM), etc.)
25. Planning, design, and implementation of new and improved information systems to meet the business requirements of customer organizations
26. Karaf, Apache ServiceMix, Camel
27. CXF platform,
28. WebSphere
29. Open source enterprise service bus (ESB)
30. Operating systems (Linux, Windows Server, AIX, etc.)
31. LAN, WAN, and backbone network services
32. Training and supporting users with custom or packaged applications and desktop platform technical support, including development of training materials and documentation

OFFEROR RESPONSE

Interested vendors should include in their response:

1. Staff qualifications
2. Cost per hour