

11.2 PROPOSAL SUBMISSION ATTACHMENTS

11.2.1 Attachment G4 – DARFUR Contracting Act Certification

In accordance with Public Contract Code section 2204(a), the Bidder certifies that at the time the Proposal is submitted, the Bidder signing the Proposal is not identified on a list created pursuant to subdivision (b) of Public Contract Code section 2203 (<http://www.dgs.ca.gov/pd/Resources/PDLegislation.aspx>) as a person (as defined in Public Contract Code section 2202I) engaging in investment activities in Iran described in subdivision (a) of Public Contract Code section 2202.5, or as a person described in subdivision (b) of Public Contract Code section 2202.5, as applicable.


Bidders are cautioned that making a false certification may subject the Bidder to civil penalties, termination of existing contract, and ineligibility to bid on a contract for a period of three (3) years in accordance with Public Contract Code section 2205. Bidder agrees that signing the DARFUR Contracting Act Certification Form shall constitute signature of this Certification.

CalSAWS M&O Services RFP #01-2022

Darfur Contracting Act Certification

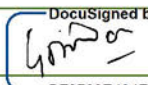
Pursuant to Public Contract Code section 10478, if a Bidder or Contractor currently or within the previous three years has had business activities or other operations outside of the United States, it must certify that it is not a "scrutinized" company as defined in Public Contract Code section 10476.

Therefore, to be eligible to submit a bid or Proposal, please complete only one of the following three paragraphs (via initials for Paragraph # 1 or Paragraph # 2, or via initials and certification for Paragraph # 3):

Initial	Attestation
	We do not currently have, or we have not had within the previous three years, business activities or other operations outside of the United States.
	We are a scrutinized company as defined in Public Contract Code section 10476, but we have received written permission from the Department of General Services (DGS) to submit a bid or Proposal pursuant to Public Contract Code section 10477(b). A copy of the written permission from DGS is included with our bid.
	We currently have, or we have had within the previous three years, business activities or other operations outside of the United States, but we certify below that we are not a scrutinized company as defined in Public Contract Code section 10476.

CERTIFICATION For # 3

I, the official named below, CERTIFY UNDER PENALTY OF PERJURY that I am duly authorized to legally bind the prospective Contractor/Bidder to the clause listed above in # 3. This certification is made under the laws of the State of California.

Contractor/ Firm Name	Accenture LLP		
By (Authorized Signature)			
Printed Name and Title of Person Signing	Gaurav Diwan, Managing Director, Accenture LLP		
Date Executed	December 9, 2022	Executed in County of	Sacramento

11.2.2 Attachment G5 – Certificate of Firm Status

The Bidder shall attach either a copy of the Certificate of Status issued by California's Office of the Secretary of State, or a copy of the firm's active on-line status information downloaded from the California Business Portal Website. If the required documentation cannot be supplied, the Contractor must document an explanation.

Accenture Response:

As requested, we provide a copy of Certificate of Status issued by California's Office of the Secretary of State on the following page.

State of California
Secretary of State

**CERTIFICATE OF GOOD STANDING
FOREIGN LIMITED LIABILITY PARTNERSHIP**

I, SHIRLEY N. WEBER, PH.D., Secretary of State of the State of California, hereby certify:

That on the **28th day of November, 1995, ACCENTURE LLP**, a limited liability partnership organized and existing under the laws of **Illinois**, complied with the requirements of California law in effect on that date for the purpose of registering to transact intrastate business in the State of California;

That the above limited liability partnership is entitled to transact intrastate business in the State of California as of the date of this certificate subject, however, to any licensing requirements otherwise imposed by the laws of this state; and

That no information is available in this office on the financial condition, business activity or practices of this limited liability partnership.

IN WITNESS WHEREOF, I execute
this certificate and affix the Great Seal
of the State of California this day of
December 14, 2022.



A handwritten signature in black ink, appearing to read "Shirley N. Weber", is written over a horizontal line.

Shirley N. Weber, Ph.D.
Secretary of State

CalSAWS M&O Services RFP #01-2022

12.4 ATTACHMENT A4 – INFRASTRUCTURE STATEMENT OF COMPLIANCE WITH REQUIREMENTS

By completing and signing this form the Bidder confirms that it:

- Read the individual Infrastructure Requirements, **Attachment A2 – Infrastructure Requirements Matrix**.
- Understands each individual Infrastructure Requirement.
- Agrees to comply with each individual Infrastructure Requirement.

By completing and signing this form, the Bidder also acknowledges that SCRs will continue to be applied to CalSAWS during the process of conducting this solicitation and the Transition Phase of the resultant Contract and agrees to take responsibility of, and comply with, all Infrastructure requirements at the time the incumbent Contractor ends or upon the request of the Consortium Executive Director or designee.

The Bidder shall complete and include this form in their response in accordance with Section 6 - Proposal Structure and Submission. Failure to sign this certification may result in the Proposal being deemed nonresponsive.

SIGNATURE & DATE	DocuSigned by:  December 9, 2022 BF8709E434EB4A5...	
NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	Gaurav Diwan, Managing Director, Accenture LLP	
COMPANY NAME	Accenture LLP	
COMPANY ADDRESS	Accenture LLP 1610 R Street, Suite #240 Sacramento, CA 95811	

CalSAWS M&O Services RFP #01-2022

12.4 ATTACHMENT A4 – INFRASTRUCTURE STATEMENT OF COMPLIANCE WITH REQUIREMENTS

By completing and signing this form the Bidder confirms that it:

- Read the individual Infrastructure Requirements, **Attachment A2 – Infrastructure Requirements Matrix**.
- Understands each individual Infrastructure Requirement.
- Agrees to comply with each individual Infrastructure Requirement.

By completing and signing this form, the Bidder also acknowledges that SCRs will continue to be applied to CalSAWS during the process of conducting this solicitation and the Transition Phase of the resultant Contract and agrees to take responsibility of, and comply with, all Infrastructure requirements at the time the incumbent Contractor ends or upon the request of the Consortium Executive Director or designee.

The Bidder shall complete and include this form in their response in accordance with Section 6 - Proposal Structure and Submission. Failure to sign this certification may result in the Proposal being deemed nonresponsive.

SIGNATURE & DATE	DocuSigned by:  December 9, 2022 BF8709E434EB4A5...	
NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	Gaurav Diwan, Managing Director, Accenture LLP	
COMPANY NAME	Accenture LLP	
COMPANY ADDRESS	Accenture LLP 1610 R Street, Suite #240 Sacramento, CA 95811	

12.8 ATTACHMENT A8 – INFRASTRUCTURE FIRM MANDATORY QUALIFICATIONS

The Bidder will complete the following tables detailing the firm's Minimum Experience for each Project to demonstrate the required experience. Provide the details of firm experience for the Infrastructure Support Contractor relevant to the proposed Infrastructure Support within at least the last 10 years.

Minimum Experience I-F1	
A minimum of three (3) years of Prime Contractor experience performing cloud-based operational activities including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring on two (2) Projects involving large and complex IT systems. Each of the two (2) Projects must have been completed or ongoing within the last five (5) years.	
Project #1	Contact #1
Company Name: Centers for Medicare and Medicaid Services (CMS)	Contact Name: [REDACTED]
Project Name: HealthCare.gov/Federally Facilitated Marketplace (FFM) (including FFM, FFM Bridge and FFE)	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) January, 11, 2014 through January, 10, 2027	Address: [REDACTED] [REDACTED]
Contract Duration (months): 156 months	Phone Number: [REDACTED]
Contract Amount: HHSM-500-2014-00191C: \$198,111,211 HHSM-500-2015-00246C: \$842,454,559 HHSM-500-2016-00003I/75FCMC21F0001: \$205,006,767 HHSM-500-2016-00003I/75FCMC21F0002: \$322,884,001 Total: \$1,363,449,771	Email: [REDACTED]
Describe the services provided:	

EXPERIENCE SUMMARY

As of January 4, 2023, Accenture has six years of prime contractor experience performing cloud-based operational activities for HealthCare.gov, a system that meets the definition of a large and complex IT system. Our cloud-based operational activities are ongoing through January 10, 2027, which means that our experience on HealthCare.gov **exceeds the requirement** as one of the two required projects for F1.

PROJECT DESCRIPTION

Through the 2010 Patient Protection and Affordable Care Act (ACA), new health insurance exchanges were created at both the state and federal levels. These exchanges are public-private marketplaces where Americans can securely shop for health insurance plans and apply for a tax subsidy simultaneously with multiple insurance companies. HealthCare.gov, the eligibility website for the federal exchange, is the front door for the Federally Facilitated Marketplace (FFM). Ancillary systems include FFM Bridge and Federally Facilitated Exchanges (FFE).

Technical solution

FFM is a cloud-based solution and uses a multi-tiered processing architecture, including a presentation tier optimized for multiple user interface platforms (such as laptops and mobile devices), an application tier, and a data tier. The system integrates with several COTS solutions (e.g., Salesforce and Interactive Voice Response (IVR)), which integrate with custom applications that are developed, deployed, and operated on Confluence and Red Hat software. The system was migrated to the Amazon Web Services (AWS) cloud platform in 2019 and has been running on that platform since then.

FFM connects with over 800 issuers enabling data sharing and claims processing in the cloud in compliance with CMS analytical algorithms. A feature of the FFM system is its innovative way of adapting to meet the unique needs of each of the 50 states through interfaces with health insurance companies and the IRS. Some states use the system's full functionality, and others use the system solely for essential eligibility functions. FFM consists of seven subsystems and has real-time integration with external systems (e.g., IRS, SSA, and DHS) to validate eligibility. FFM is utilized in multiple locations across the country annually by over 1,000 internal and 10 million external users to enroll in qualified health insurance plans.

Services delivered

A rescue of the website began in November 2013, and in January 2014, the federal government hired Accenture as the prime contractor for application maintenance, system modifications, cloud-based operations, project management, cybersecurity vulnerability mitigation, network and system engineering, capacity planning, performance testing and monitoring, and batch processing. In just six weeks, Accenture mobilized more than 500 skilled professionals to transition the system from the original vendor to Accenture at an unprecedented speed.

Working closely with the original vendor, Accenture quickly achieved CMS' objective to stabilize and enhance HealthCare.gov. A collaborative and comprehensive transition plan was created that mitigated the risk and enabled Accenture to begin hands-

on delivery. Within eight weeks, Accenture delivered significant technical enhancements to the website, stabilizing it during the peak of HealthCare.gov's initial enrollment period. This enabled millions of Americans to securely enroll in health insurance.

Accenture is responsible for stabilizing, securing, and improving the website, maintaining hardware/software, and developing additional systems and interfaces while managing maintenance and operations. In addition to providing issuers with a complete data processing environment, Accenture developed an innovative solution that each issuer owns and operates. The FFM modernization projects for HealthCare.gov include Accenture as the prime contractor, four other vendors responsible for different areas of the system, contractors in all 50 states, insurance companies, and the IRS.

The FFM Service Desk, a multi-tier service desk, is managed and operated by Accenture in partnership with CMS. CMS is responsible for Tier 1 support. Accenture is responsible for Tier 2 and Tier 3 support using the Information Technology Infrastructure Library (ITIL) standards and framework. Additional support services include security, maintenance, and system interoperability. More than 50,000 issues were triaged and resolved by the FFM Service Desk between 2015 and 2022.

Accenture has successfully operated through seven open and special enrollment periods in collaboration with CMS and other FFM stakeholders to support 45 million enrollments and \$200 billion in total payments since 2015. Accenture's contract has been renewed three times and is ongoing through January 10, 2027.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** FFM consists of seven subsystems that interface with each other and integrate with external systems including COTS packages like Salesforce with custom-developed components built and deployed upon software by Confluence and Red Hat. FFM's seven subsystems include Eligibility and Enrollment, Stand-Alone Eligibility, Plan Management, Financial Management, Marketplace Consumer Record, Insurance Enrollment System and the Document Storage and Retrieval System.
2. **Interfaces with at least five external systems, at least one of which is real-time:** FFM interfaces with internal CMS components and systems external to CMS, including 27 state systems to support account transfers. FFM has real-time integrations with IRS, SSA, and DHS systems to validate eligibility via the CMS HUB. For issuer support, the System Exchange Enrollment Data application integrates with FFM. For eligibility support, the Eligibility Support system integrates with FFM for DMI/SVI adjudication. The Eligibility Support Desktop Change Utility Tool integrates with FFM to assist with appeals and eligibility determinations of consumers. The Next Generation Desktop integrates with the FFM for call center support. For issuer payment, it interacts with CMS' HIGLAS general ledger and payment system.
3. **Is accessed by at least 1,000 users at multiple locations:** FFM is used by over 1,000 internal users and 10 million consumers annually to enroll in qualified health insurance plans across 34 states.
4. **Has a contract value of at least \$10,000,000 dollars:** The FFM contract value is \$1.36 billion over 13 years.

5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:

The FFM solution includes multi-tiered processing, including online, API-based, and batch processing, with data integration for internal and external partners. FFM is highly tuned to support evolving consumer needs—the customer facing front-end is optimized for multiple user interface platforms. Accenture conducts significant performance testing and tuning in close collaboration with CMS to ensure FFM is aligned with CMS' objectives for each open enrollment period.

I-F1 EXPERIENCE DETAILS

Accenture's involvement in infrastructure operations with HealthCare.gov began in November 2013 and, by January 2014, the federal government hired us as the prime development and infrastructure contractor for operating the service's deployment on AWS cloud. Our cloud-based operational activities include network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring.

Cloud-based operations

The new federal and state health insurance exchanges created new marketplaces for insurance companies to sell products to new consumers. To stabilize the pricing of risk, the ACA included new reinsurance and risk adjustment programs. The former helped offset larger-than-expected claims, and the latter helped transfer payments from issuers that took on lower-than-expected risk to those that took on higher-than-expected risk. These programs required gathering confidential claims information from 800 different insurance issuers and then performing complex, risk stabilization calculations and analytics. CMS needed to provide a solution where issuers maintained control of their confidential claims information, as input to the risk calculations, but CMS controlled the risk algorithms, software, and reference data.

Our services included stabilizing and improving the cloud-based web infrastructure and completing the development of the additional systems and interfaces. Accenture developed an innovative solution that provides issuers a cloud-based environment, which each issuer operates. The "EDGE" system uses AWS cloud to connect with more than 800 issuers to share and process claims information in the cloud according to the CMS analytical algorithms. Within eight weeks, Accenture delivered significant technical improvements to the website, stabilizing it during the peak of HealthCare.gov's initial enrollment period.

Issuers maintain complete control of their proprietary claims and pricing data and CMS only has visibility to the outputs of the algorithms. Additionally, 135 issuers elected to participate on AWS-deployed servers, using a fully automated environment-provisioning process that successfully and securely processed the issuers' data without requiring an internal infrastructure investment. The other issuers used an on-premises deployment model, which still took advantage of the same software images and upgrade processes. The EDGE system enables CMS to create a level playing field for all issuers. It provides consistent software and data version management across the universe of independent installations. EDGE simplifies and expedites deployment for issuers, reducing deployment time from several days in a standard software distribution and configuration model to as little as 15 minutes, while enabling hands-free software upgrades and execution of remote commands.

The EDGE software delivery was not the only use of the cloud. Accenture took a "cloud first" approach, using the cloud when optimal to meet CMS' security needs. For example, the suite of automated, fully scalable, functional tests is run from servers in the cloud. Additionally, new environments for new software capabilities are deployed in AWS. This approach automated the provisioning of new environments, COTS middleware, and the application software.

Another example is cloud-based DevOps. Accenture implemented full DevOps processes and technologies in the cloud to accelerate development and deployment. Automated tasks across environments include code check-out, build and packaging, code quality scanning, security scanning, unit testing, functional testing, and initial performance testing, software deployment, and release smoke testing.

The team used tools such as Junit, GitHub, Amazon Web Services, JIRA Software (including Jira, Confluence and HipChat), Python Bash to support continuous delivery, and an industry-proven tool to protect the security of FFM APIs, Code, Containers, and applications. Given differences in on-premises and cloud services, Accenture manually reconfigured critical monitoring tools during the migration to AWS. We closely coordinated with CMS and other vendors during multiple onsite meetings to manually modify, export, and conduct validations on approximately 70 dashboards (e.g., updated approximately 300 alerts, search field changes) to ensure compatibility with AWS. Additionally, the team developed and shared detailed user guides with key stakeholders outlining reconfiguration requirements and actionable next steps to inform any future dashboard migration activities. The DevOps approach has significantly reduced manual errors, improved software release quality, and allowed the team to deliver faster.

Operations monitoring

Our approach for cloud-based business operations general support meets issuer and consumer needs and correctly processes approximately 20 million applications and approximately 8.4 million enrollments each year. We do this through 24/7 system monitoring, mature alerting processes, and tiered incident responses based on statements of procedures (SOP). We utilize early-warning monitoring alerts of operational anomalies before they affect system performance. Our early-warning alerts are based on threshold assessments continuously reviewed and revised to enable accurate alerting. We work collaboratively with CMS people and organizations on approximately 10,000 operational requests and incidents annually. Using our processes, tools, and skilled resources, we provide insight and analysis for troubleshooting and provide FFE organizations with clear recommendations to address emerging issues, even when the issue belongs to another area.

Operations security

We continuously monitor FFE operations for compliance, advanced threat protection, and fraud vulnerabilities using our security methodology, including monitoring, assessment, and communication approach is aligned to the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). We perform security impact assessments and vulnerability scans for all new capabilities. We collaborate with CMS to implement and revise pre-defined plans and actions to escalate detection of

potential security and privacy issues. Our security and privacy approach has been demonstrated to support four Authority to Operates (ATO)s, more than 1,600 monitoring alerts, and 1,100 security tickets annually.

Network engineering

Accenture employs skilled technology architects, functional experts, infrastructure engineers, and professional business analysts who bring industry-proven practices, reusable technology frameworks, and strong architecture principles. The site infrastructure and its associated networking are on AWS. We have configured networking components on AWS, including Virtual Cloud Networks (VCNs), Load Balancers, DNS Management, and IP Management. We engineered and maintained a network infrastructure designed to sustain high levels of availability for county and remote users. This infrastructure maintenance configuring enables physical and virtual networks, network security, and high availability. All network design changes align with Federal policy. We plan new initiatives and expand the existing network infrastructure in-line with the migration; provide and implement solutions based on issues such as traffic congestion, infrastructure upgrades, and routine troubleshooting; document solutions/blueprints for any network-related risks or issues; install any hardware or software; create back-ups for all systems; and monitor the system performance. We have maintained a 99.8% uptime success rate with minimum impact to availability.

Cybersecurity vulnerability mitigations

Accenture's management of security operations services includes threat detection, monitoring, scanning, security incident process management, vulnerability scans, and auditing. Accenture employs system monitoring automated mechanisms using industry alert and monitoring tools to integrate audit review, analysis, and reporting. These activities support organizational processes for investigation and response to suspicious activities. Accenture analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

FFM servers generate system logs which contain event entries for all system level actions. The FFM Mark Logic database provides a logging function. User authentication and user actions/events are created in local logs for FFM OPS managed accounts such as administrative accounts at the server and database levels, or administrator accounts on the server middleware layer. On the database layer, Mark Logic records log events. This makes it possible to reconstruct which user accessed which files or database records. AWS S3 CloudTrail and Scalable Login Service include detailed information in the audit records.

Results from vulnerability scans are on the CMS Virtual Private Cloud and scans provided by AWS are used to drive patching and other remediation for FFM. In addition, Accenture performs both static and dynamic application scanning to detect vulnerabilities. Accenture minimizes false positives with these scans by executing safe versions of exploits, allowing developers to focus on findings that require action. Data from the scans is also used for trend analysis and executive reporting.

We use cloud threat detection tools to monitor the overall AWS Cloud security posture and surveil for malicious activity and anomalous behavior. Our team reviews events and alerts to determine the proper course of action. Accenture also performs security assessments to identify potential threats. We verify the systems are secure and do not have vulnerabilities that can potentially weaken their security posture.

Accenture uses other tools for logging, security monitoring, and auditing. On the FFM application side, Accenture built logging and auditing capabilities for all transactions, which feeds into other monitoring tools. Accenture also sets up custom filters and thresholds to get alerts for events such as the potential transfer of sensitive data or high numbers of calls to certain APIs. Our monitoring tool includes specifications of log types and source systems that are candidates for log capture and management. Using our security tools, Accenture links access to system components to individual users for networking equipment and servers. Infrastructure audit records include user identification, event type, date and time stamp, success or failure indication, origination of event, and name or identity of affected data, system component, or resources. Accenture's performance of these activities protects CMS' information from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional.

Through this program, we have completed all required external audits (e.g., IRS, FISMA) and penetration tests with no high or critical findings. A few findings and PoA&Ms of lower criticality were promptly remediated and closed. We have successfully maintained a strong security posture for the FFM application and continuously achieved Authority to Operate (ATO) on schedule for the systems that Accenture built and maintains.

Capacity planning

Our capacity management and planning approach uses a baseline capacity map for FFE services, which documents component capacity, expected usage, and performance requirements. As modified or enhanced capabilities are being planned, we evaluate their expected performance impact. We identify adjustments to maintain required performance and capacity, obtain CMS approval, and schedule through the standard CMS release management processes. We conduct regular performance tests to validate FFE capacity and performance requirements are met. We collaborate with CMS and other FFE organizations for release oversight using standard processes and tools and use tailored risk and escalation processes for release-related risks.

Our approach to align release plans with industry best practices is grounded in our use of these practices for software release and deployment management in alignment with CMS standards, including SAFe Agile. We evaluate new technology at least quarterly to improve FFE performance, operability, portability, elasticity, resilience, and agility.

We use information from our pre-defined action plans and monitoring teams to rapidly identify the code or configuration changes required for resolution. Accenture's rapid response approach and use of a cross-skilled monitoring team enables immediate response to CMS and assistance to other Application Development Organizations (ADO)s, to help minimize risk to FFE operations. Successful operation of FFE requires that the system maintain maximum availability for users. Our overall approach for software release and deployment management delivers maximum system availability through disciplined and collaborative processes.

Performance testing

Accenture conducts performance testing to evaluate the speed, responsiveness, and stability of the application under a simulated user workload. Before open enrollment (OE), we conduct performance testing at varying loads as well as targeted performance testing for peak operational periods in a production-like environment. We then execute performance testing in a real production-sized environment with production-level data to meet and exceed expected consumer traffic volumes against the system without impacting production data. For example, we conduct extensive pre-OE performance testing, including tabletop exercises, resiliency testing, and simulated system failure drills. Our performance testing approach proactively identifies potential FFE anomalies and allows us to prevent OE issues and rapidly remediate issues, working with cross-exchange participants and improving consumers' OE experience. The insights from these performance tests are used to deliver new enhancements ahead of peak traffic (e.g., query tuning, data cleanups, infrastructure scaling).

We analyze the production-sized performance test results against Accenture and CMS-approved service level agreements to identify and remediate potential issues. Based on CMS approval, our recommendations are implemented in FFE or other FFE participant infrastructure, databases, and applications to resolve performance related concerns.

We review and provide guidance to external vendors on testing models and results and explain our data modeling techniques to teach vendors about the significant performance impacts for specific data and use cases. This improves understanding of cross-exchange performance behaviors and enables critical observations of application, business, and infrastructure performance during peak system load and yields risk-mitigating actions.

Exceptional production monitoring detects potential issues (ours and other vendors) and allows us to resolve them before they have impact. Exceptional performance testing allows CMS to right-size cloud infrastructure enabling stable operations at the lowest needed cost.

Rescuing the HealthCare.gov website required immediately instilling technology discipline, along with significant investments in automation and tooling. To improve the fully manual test and release process, the Accenture team created fully automated, regression test suites at all levels, including:

- 15,500 unit test cases in Java
- 1,400 functional tests, end-to-end, for the user interfaces
- 15,400 functional data validation and batch validation tests
- 990 transactions tested in a comprehensive, end-to-end performance suite, reflecting a real-world transaction mix

This comprehensive regression suite runs on a regular basis and provides automated emails and executive dashboards for monitoring. The automated functional testing consists of more than 300,000 test steps and is typically executed five times per week. The automation of this functional testing saves over 50,000 hours per year in manual testing. This high level of automation has allowed the team to dramatically improve the quality, reliability, and speed of new software builds.

Performance monitoring

Our approach for 24/7 continuous monitoring uses an integrated monitoring toolset to generate early-warning alerts of potential issues. We provide a full view of application and system performance and share alerts with our Tier 1 support team and potentially affected Application Development Organizations (ADO)s. We rapidly and collaboratively analyze anomalies and use pre-defined action plans to determine and remediate the root cause. We have more than 2,800 early-warning alerts, each with a pre-defined action-plan to accelerate analysis and remediation actions for quickly implementing fixes.

We use monitoring insights to create dashboards that tie multiple monitoring data sources together and provide an integrated view of FFE monitoring. We create, maintain, and share a set of high-level dashboards for an overview of system performance and stability. These dashboards trend with an even larger suite of dashboards to display more granular data critical to rapid triaging. We also share over 200 fine-grained dashboard variations across database, network, security, and cross-exchange monitoring categories.

We use ticket tracking services to monitor issue troubleshooting and inquiry progress and further support resolution communication using a real-time messaging platform to provide ticket updates and collaborate with key stakeholders. During peak periods, such as OE, we also utilize 24/7 eyes-on-glass, on-site monitoring and meet with key stakeholders daily to effectively manage system load. Our on-call resources have the breadth and depth of skills to detect and act on any unexpected system variations.

Project #2	Contact #2
Company Name: U.S. Department of Treasury Internal Revenue Service	Contact Name: [REDACTED]
Project Name: Integrated Enterprise Portal (IEP) 1.5 Program	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) IEP 1.0 May, 19, 2011 through May, 18, 2017 IEP 1.5 February, 15, 2017 through February, 14, 2025	Address: [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 164 months	Phone Number: [REDACTED]
Contract Amount: Exceeds \$1,000,000,000	Email: [REDACTED]
Describe the services provided:	

EXPERIENCE SUMMARY

As of January 4, 2023, Accenture has five years and 10 months of prime contractor experience performing cloud-based operational activities including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring for Federal Treasury Integrated Enterprise Portal (IEP), a system that meets the definition of a large and complex IT system. Therefore, our experience on the Federal Treasury IEP **exceeds the requirement** of three years as one of the two projects needed for F1.

Project Description

The IEP 1.5 Program is the digital front door to the Internal Revenue Service's (IRS) backend systems and provides technology services to thousands of internal and external users. It is mission critical in securely serving taxpayers, tax preparers, and employees. By continuously improving and innovating its platforms and applications through the IEP 1.5 Program, the IRS is sustaining its infrastructure and applications, expanding capabilities, and increasing resiliency.

Initially transitioning two portals from another contractor, Accenture's involvement with the IEP began in May 2011 on the IEP 1.0 Program. In February 2017, Accenture partnered with the IRS on the IEP 1.5 Program to perform maintenance and operations of its infrastructure and applications.

Technical solution

A key component of the IEP 1.5 infrastructure is its ability to deliver a scalable, elastic infrastructure using cloud-based services. The IEP infrastructure is designed to support iterative transformation without service disruption. IEP 1.5 encompasses the following systems and domains:

- Public User Portal (PUP – IRS.gov)
- Registered User Portal (RUP)
- Employee User Portal (EUP)
- Portal Account Replacement Tool (PART)
- Affordable Care Act Transactional Portal Environment (ACA-TPE)
- Certified Professional Employer Organization (CPEO) & 501(c)(4) Online Registration System
- Field Assistance Scheduling Tool (FAST)
- 90+ managed applications
- 3,500+ servers

The IEP features a multi-tiered processing architecture, including three user portals optimized for multiple user interface platforms (e.g., laptops and mobile devices). As part of the IEP solution, Accenture integrated over 90 applications, including ServiceNow

and CPEO Versa, both of which are COTS applications. Accenture has also integrated five external systems, including the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.

The modernized system is accessed by over 1,000 internal users from multiple locations. During the 2021 filing season (February 12 to May 17, 2021), there were 767.1 million total site visits (from internal and external users) to IRS.gov and 2.02 billion page views on the site. The peak day was March 15, 2021, when 37.3 million visited the site and 88.1 million pages were viewed.

Services delivered

As the prime contractor, Accenture uses AWS cloud services for production applications and manages more than 40 public applications. Accenture is responsible for system modifications, hardware/software, project management, and cloud-based operations activities such as network and system engineering, cybersecurity vulnerability mitigation, capacity planning, performance testing and monitoring, and batch processing. Accenture also supports security, maintenance, and interoperability. The large and complex Federal Treasury IEP Program contract value exceeds \$1 billion and is ongoing through February 2025.

Using the Information Technology Infrastructure Library (ITIL) as the service desk framework, Accenture provides Tier 1 and Tier 2 service desk support for the IEP non-production environments. The IEP service desk supports request fulfillment, incident management, problem management, and asset management. Additionally, the IEP service desk provides initial support for all IEP-related incidents, including opening tickets in the ITSM system to coordinate with other IRS organizations for incidents outside of the IEP purview.

Accenture created the IRS.gov website Help Desk, which serves as a "first aid station" for IRS.gov website questions such as navigation of IRS content and forms retrieval. The IRS.gov website Help Desk is a complementary service to the IRS toll-free tax assistance line. Accenture successfully delivered the IRS.gov website Help Desk for the IRS for 15 years and acted as the front door for many IRS.gov website visitors in their interactions with IRS.

Accenture collaborates in a multi-contractor environment with five other contractors responsible for different areas of the IEP. Accenture works with contractors such as Leidos, Deloitte, and Booz Allen to manage and maintain the IRS' infrastructure and coordinate the five legislatively mandated applications currently under development in the IEP's AWS-managed service cloud (two of which are Accenture-managed). Accenture is currently migrating legislatively mandated applications to the cloud and is expected to complete the migration of the remaining applications by January 2023.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The IEP solution integrates with over 90 applications. ServiceNow and CPEO Versa are two of the top COTS applications. In addition, PART is a care act identity management COTS product and FAST is the ServiceNow COTS product.

2. **Interfaces with at least five external systems, at least one of which is real-time:** The IEP solution interfaces with five external systems, hosted by Health and Human Services for Medicare & Medicaid Services (HHS CMS) and IRS back-end systems. The applications include but are not limited to the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.
3. **Is accessed by at least 1,000 users at multiple locations:** The IEP solution is accessed by more than 1,000 users at multiple locations. The PUP—the IRS external or internet portal, IRS.gov, that allows unrestricted public access to non-sensitive materials and applications had 2.02 billion page views and 767.1 million total visits during the 2021 filing season (February 12–May 17, 2021).
4. **Has a contract value of at least \$10,000,000 dollars:** The IEP solution contract value exceeds \$1 billion.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The IEP solution features multi-tiered processing, including a user facing front-end optimized for multiple user interface platforms. There are three main portals: PUP, registered user portal, and employee user portal. The ACA Application-to-Application (A2A) is a core interface.

I-F1 EXPERIENCE DETAILS

Accenture's involvement in infrastructure operations with the IEP began during the IEP 1.0 project in May 2011, but cloud-based operations planning began with the start of IEP 1.5 in February 2017. In 2017, Accenture partnered with the IRS to perform maintenance and operations of its infrastructure and applications. As part of this initiative, Accenture and the IRS built a redesigned IRS.gov website using the newly implemented cloud-based web content management system (WCMS) hosted in Acquia (AWS). The redesigned website is mobile friendly and includes a cloud-based enterprise search capability. IEP 1.5's PUP Web Application Services transitioned all the PUP applications from the legacy dedicated PUP infrastructure to the shared IEP infrastructure. In November 2019, Accenture transitioned approximately 20 PUP applications to AWS GovCloud. As of April 2021, the PUP hosts 28 applications, ranging from estimators, tax assistants, and site utilities. 23 of the 28 hosted applications are fully managed by Accenture. Our cloud-based operational activities with the IEP include network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring, and are ongoing through February 2025.

Cloud-based activities

Accenture's long-term collaboration with the agency dates back more than a decade. For IEP 1.5, Accenture serves as the agency's strategic infrastructure services provider. As part of managing cloud and on-premises infrastructure operations, our services include:

- Patching of various hardware and software components
- Performing vulnerability scanning

- Updating antivirus on daily basis
- Executing technical changes
- Managing change
- Monitoring the infrastructure components for errors
- Performing error handling and corrective actions
- Supporting auditing solution and reporting
- Monitoring and tuning performance
- Creating runbooks and job aids
- Managing capacity and reporting
- Managing user access
- Managing assets and configurations

Accenture is the prime contractor for IRS Treasury cloud IaaS support. The Accenture team was contracted to design, build, and implement Nethub, and manage initial operations after go-live. Accenture built the Nethub infrastructure within the IRS Treasury cloud instance of AWS GovCloud in May of 2020. The Nethub cloud environment was designed as an enterprise-wide solution to provide a set of core services, such as management, network, security, identity, compliance, and governance to downstream cloud workloads. The Nethub core services were built across multiple Virtual Private Clouds (VPCs) within the Nethub account, which include the following:

- Transit Hub VPC (secure network connectivity and routing)
- Security VPC (platform security, audit and compliance controls, secure log aggregation, and retention)
- Management VPC (software images, backup and restore functions, infrastructure build, patching, and monitoring tools)
- Common Services VPC (continuous integration and continuous deployment (CI/CD) pipeline tools)
- Logging VPC (AWS logging tools, Syslog sources, and universal forwarders)

In addition to the initial build and integration tasks for each VPC, there was a notable effort that involved working with IRS Security and IRS Splunk stakeholders to design, build, and integrate a solution consisting of Splunk forwarders in the Logging VPC to also forward all AWS Splunk logs to IRS on-premises Splunk indexers.

Other key Accenture activities included the following:

- Holding multiple design sessions with key client stakeholders and SMEs within ES, EOps, CyberSecurity, and UNS to develop design documentation, such as the Nethub Simplified Design Specification Report (SDSR), the Interface Control Document (ICD), and a Computer Operator Handbook (COH)

- Developing Nethub security documentation, such as the Nethub System Security Package (SSP) and other security plans, supporting security activities such as the CPO (FedRAMP) Assessment, obtaining authorization to operate (ATO) for both Nethub Release 1 and Release 2, and integrating with IRS configuration compliance tools (BigFix and CASB) and IRS vulnerability tools (Nessus) to remediate findings in accordance with the timeline noted in the Internal Revenue Manual (IRM)
- Supporting the cloud organizational readiness activities by developing and implementing the Day 1 Cloud Operations Model for Nethub. Multiple interviews were held with EOps, UNS, and CyberSecurity divisions to understand current on-premises processes and then create appropriate processes for cloud. These processes now take place in O&M and are noted here:
 - Cloud core services change management (implementation in progress)
 - Incident management and security
 - Server build and access management
 - Monitoring and patch management
 - Infrastructure configuration and asset management
 - Cloud tagging
 - User support and knowledge management

Network engineering

The IEP uses a mixture of AWS Cloud and on-premises networking solutions. We engineered and maintained a network infrastructure designed to sustain high levels of availability and security. This infrastructure includes maintenance configuring physical and virtual networks, network security, and high availability. All network design changes align with Federal policy. We engineer designs for all new initiatives and expand the existing network infrastructure in line with the migration. We provide and implement solutions based on issues such as traffic congestion, infrastructure upgrades, and routine troubleshooting. We document solutions/blueprints for any network-related risks or issues, and install any hardware or software, create back-ups for all systems, and monitor the system performance. We maintained over a 99.99% network uptime success rate with minimum impact to availability.

Cybersecurity vulnerability mitigations

The IEP infrastructure must mitigate security threats to IRS assets and protect taxpayer data, including mitigating threats to the AWS Cloud. Accenture provides Edge security for IEP web applications via web application firewalls, client IP blocking, bot management, and log analytics. Accenture has worked closely with IRS Cybersecurity to identify, develop, and tune security technologies enabling rapid response to fraud activity and blocking of potential bad actors from executing attacks against IRS web applications. Tuning and queries on the near-real time data that the IEP ingests provide advanced security monitoring and analysis capabilities for identifying external application-level attacks, classification of end users, and active bot detection.

Accenture has been providing services to the IRS using the National Institute of Standards and Technology (NIST) Risk Management Framework for over 10 years. The systems we manage are compliant with the security policies. Additionally, we have successfully gone through the FedRAMP Agency Authorization process to obtain ATOs for multiple IRS cloud applications.

Accenture monitors industry and government sources for information on new and emerging threats. As these emerging threats are identified, we evaluate their applicability to the IEP 1.5 solution. When applicable, we update the overall Portal threat model and use our various security tools to determine if the threat is present in the on-premises and cloud environments. Once the threat is confirmed, the IEP 1.5 Security team evaluates the options for prevention and works with the IRS to determine the next steps for the implementation.

Accenture supports vulnerability scanning, penetration testing, and independent validation and verification (IV&V) of security controls for applications hosted on the IEP 1.5 platform. There are three primary phases to IEP's approach to manage vulnerabilities: identification, prioritization, and patch deployment. For identification, we use multiple security tools and notifications from IRS Security or other third parties. For prioritization, Accenture uses a risk matrix (outlined in the Internal Revenue Manual) that provides a customized risk score based on various inputs. Patch deployment is based on the results of prioritization. Accenture completes the development, testing, and deployment of patches in the timeframes defined.

Capacity planning

Our capacity management approach includes providing the IRS with a direct line of sight to the operational data that drives costs. Capacity management emphasizes transparency through access to tools that analyze capacity usage. Accenture conducts periodic analysis of the capacity allocation and usage. The results and right-sizing recommendations are provided as monthly, quarterly, and annual reports to the IRS. Individual application usage reports are provided to the application owners to help with capacity forecasting. Through the IEP Service Catalog, users can request new application provisioning, modifications, and provide capacity forecasts. The Service Catalog workflow is incorporated into the IRS Technical Review Board (TRB) process and handles service requests and their associated demands for capacity.

Capacity management has three main objectives:

- Maintain a 25% of the baseline capacity as buffer. Accenture tracks the IEP allocated capacity and confirms a 25% buffer is maintained. This is done through weekly reporting and reviews covering storage, CPU, memory, and software licensing. Actions are initiated as needed to address situations where the buffer is at risk. Baseline and buffer usage are reported in the quarterly reports to the IRS.
- Determine business demand to understand the growth needs of the system. Accenture collects capacity forecasting information from application owners on a quarterly basis and matches with existing IEP capacity usage to ensure applications are provided with the required resources.

- Understand the performance and utilization of infrastructure components and their potential impacts to capacity. Accenture analyzes the application capacity usage on a weekly, monthly, and quarterly cycle and provides recommendations to right-size the capacity allocations.

Capacity management emphasizes analytics-based predictions of the behavior for IEP 1.5 services. This allows us to provide an estimate of expected changes in required capacity. Key performance indicators (KPIs) are defined and updated to maintain model accuracy. We provide capacity metrics across IEP services, including virtual machine environments, server types (e.g., application servers and database servers), storage, and network bandwidth. These details are included in the monthly and quarterly capacity reports and reviewed with the IRS. Additionally, the capacity forecasting and right-sizing information is discussed with application owners to take appropriate action.

All IEP hosting environments meet a set of minimum characteristics including broad network access, resource pooling, rapid elasticity, and measured service with metering capabilities. All hosting environments were created with an understanding of the need for secure network connectivity to the IRS network. Accenture provides secure redundant network connectivity between the primary and secondary IRS facilities and the IEP facilities using firewalls and secure/encrypted communication protocols. All IEP 1.5 on-premises and cloud environments support the capability of dynamically assigning physical and virtual resources to support the IEP 1.5 stakeholder demands. IEP resources can elastically be provisioned and released to rapidly increase and decrease in scale to support IEP demand. Accenture also provides the ability to measure and meter services to manage the service usage of the IEP environments. Some specific results of our capacity management solution include the implementation of a new, solid-state disk storage as IEP's primary new storage solution and the build-out of a new backup storage solution to replace the outdated legacy system.

Performance testing

Our Application Infrastructure Integration Services (AIIS) team is the support team that works with the IRS to help correctly configure IRS-owned applications to run on the IEP cloud and on-premises platform. AIIS has a variety of responsibilities from performance tuning, application deployment, incident response and onboarding, configuration and troubleshooting, shared service support, and engineering services. Accenture also implemented an Application Performance Monitoring (APM) tool in the IEP. We use this tool to provide the IRS and IEP with detailed views into application transaction times for applications hosted in the IEP. This helps triage performance degradation issue resolution more quickly during incidents.

For application performance tuning, AIIS works with application owners to ensure the application runs efficiently on the IEP platform. The team supports tuning across the entire IEP 1.5 cloud and on-premises platform (web, application, database, middleware, logging, security, network, and appropriate interfaces). To support application performance testing and tuning activities, AIIS provides a standardized performance test environment (PETE). This environment is part of the migration path to production and includes test frameworks and tools to facilitate execution of these activities. Along with performance testing, the

AIS team works with application owners to evaluate configurations and performance to identify and address potential performance issues.

Performance monitoring

Our infrastructure monitoring capability watches the performance and availability of infrastructure and cloud services, including servers, applications, web transactions, and storage systems, to support infrastructure uptime requirements. Early event detection enables the support team to set priorities and respond to events before they affect business processing or taxpayers. Monitoring combined with our solution of redundant systems, active/active data centers, multiple communications paths, virtualization, and high availability capabilities are used to proactively address infrastructure failures that would influence response and availability.

We use a variety of monitoring and operational tools for IEP cloud and on-premises services and expanded their use to consolidate monitoring data and provide better visibility and analytics. IEP's 24/7/365 monitoring of the entire platform, from the infrastructure through the application layer, assesses the availability, reliability, performance, security, and the health of IEP cloud and on-premises components and associated applications with the following:

- External monitoring of applications and websites that replicate end user experience
- Internal monitoring of connectivity between edge caching and origin infrastructure
- Internal, bottom-up infrastructure alerting, monitoring, and reporting of applications, bandwidth, databases, operating systems, networks, servers, middleware components, and websites
- Health, capacity, and performance monitoring and alerting of the virtual infrastructure
- Security monitoring and assessment capabilities
- Increased integration with IRS backend monitoring tools monitoring traffic flow between the IEP and the IRS backend

To define potential problems based on the data collected from monitoring tools, we use KPIs, thresholds, and monitoring events. There can be several reasons for triggering an event, such as exceeding a capacity KPI threshold, encountering an operating system warning, performance degradation, or component failure. The actions taken upon triggering an event depends on the severity or significance of the event. Our monitoring process includes triggering alerts when there are more serious events, such as warnings. Processes are also put in place for multiple related alerts to trigger the incident management process. Tickets are generated and tracked in the IRS' ITSM tool and alerts are escalated to on-call staff for diagnosis and corrective action. We also have an after-hours service desk for the IRS to report issues.

Accenture proactively leads and coordinates problem management investigation for issues that reside within the IEP. We coordinate problem management activities with the IRS Problem Management ownership group and support any issues for which we are not an owner as needed. In addition to our successful ITIL-based incident management process, the IEP is continuously improving incident and problem management capabilities. Application performance monitoring (APM) has since been implemented, allowing for additional more rapid incident resolution to ensure the IEP meets the revised Priority 2 (P2) resolution time service level objectives (SLOs). An alert management tool has been implemented to assist with managing alerts and pooling

of resources to support Priority 1 (P1) and P2 incident response SLO times. Working in conjunction with IEP monitoring and alerting tools, the Accenture IEP Service Desk (IEP SD) serves as the main facilitator for our Incident and Problem Management processes. The SD uses the IRS Incident Management process to coordinate larger responses and notify IRS stakeholders as needed throughout an incident's lifecycle from identification, through troubleshooting to closure. The IEP SD works with support resources to triage, provide an issue ownership acknowledgment, and coordinate larger responses as need. Additionally, the IEP SD uses an ITIL-based problem management process that addresses recurring minor incidents and works to identify root causes for high priority incidents.

Specific results of our performance monitoring solution as of April 2021 include:

- Implemented an APM tool in the IEP
- Acceptable Quality Level (AQL) since the inception of the program:
 - Average P1 incident time to respond SLA is 15 minutes or less; our average is less than six minutes.
 - Average P2 incident time to respond SLA is one hour or less; our average is less than seven minutes.
 - Average P1 incident resolution time SLA is within four hours; our average is less than three hours.
 - Average P2 incident resolution time SLA is within eight hours; our average is less than four hours.
 - 95% of P1 or P2 problem management tickets assigned to Accenture shall be closed within 176 calendar days to meet SLA; we exceeded this AQL with a score of 100%.
- Amount of time between when Accenture becomes aware of an incident and when contractor notifies IRS:
 - Average P1 SLA of 15 minutes or less; our average is less than 1 minute.
 - Average P2 SLA of 1 hour or less; our average is less than 4 minutes.

Project #3	Contact #3
Company Name: California Statewide Automated Welfare System (CalSAWS) Consortium	Contact Name: [REDACTED]
Project Name: California Statewide Automated Welfare System (CalSAWS) (prior project name was the LEADER Replacement System (LRS), which is now called CalSAWS)	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) LRS/CalSAWS November 7, 2012 through April, 30, 2025	Address: [REDACTED] [REDACTED]

Cloud-based operational activities October, 14, 2019 through present	
Contract Duration (months): 149 months	Phone Number: [REDACTED]
Contract Amount: LRS/CalSAWS \$1,425,495,842	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture has three years and two months of experience performing cloud-based operational activities including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring on CalSAWS, a system that meets the definition of a large and complex IT system. Therefore, our experience on CalSAWS exceeds the requirement as one of the two projects needed for F1.</p> <p>PROJECT DESCRIPTION</p> <p>CalSAWS is an integrated eligibility system built and operated by the CalSAWS Consortium on behalf of the 58 counties of California. CalSAWS supports the counties in administering public assistance programs in California, including cash assistance (CalWORKs/TANF), food assistance (CalFresh/SNAP), medical assistance (Medi-Cal/Medicaid), and other state and county-specific programs. The system first went live in 2015 in Los Angeles County, and at that time, it was known as the LEADER Replacement System (LRS). Migration from an on-premises data center to cloud hosting occurred on October 14, 2019.</p> <p>Technical solution</p> <p>CalSAWS is the most extensive integrated eligibility system in the United States and is hosted in the Amazon Web Services (AWS) cloud. Supporting over 10 million transactions daily, CalSAWS has more than 50 interfaces, six of which are real-time. The system is currently in production in 42 counties. The system is used by 18,500 internal users daily across 125 locations to support 11 million Californians who receive public assistance. CalSAWS issues more than \$1 billion in benefits each month. By October 2023, all 58 counties will have migrated to this platform. After all counties are migrated to CalSAWS, 41,000 internal users will use CalSAWS daily to support approximately 19 million Californians and issue approximately \$2 billion in benefits each month.</p> <p>Services delivered</p> <p>Accenture is one of six contractors responsible for CalSAWS and has the largest scope of work. Accenture's contract began in November 2012 and is ongoing through April 2025. As the prime contractor for systems integration and maintenance and operations (M&O), Accenture is responsible for application maintenance and system enhancements, and cloud-based operations including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing and monitoring, and batch processing. Accenture supports hardware and software management, system engineering, data</p>	

conversion, and project management. Accenture also supports the service desk (tiers 1, 2 and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework.

Accenture is responsible for the core CalSAWS eligibility system, the analytics application, ForgeRock identity solution, contact center technologies, the Child Care Provider Portal, and kiosks/tablets in several county lobbies. The CalSAWS Consortium has separate prime contracts for the legacy system maintenance (CalWIN), cloud hosting, the public portal (BenefitsCal), imaging (SaaS contract), OCAT, GA/GR Correspondence solution, and print services.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CalSAWS solution integrates custom Java code with COTS applications (e.g., Oracle database and middleware products, Informatica Identity Resolution, Pitney Bowes Spectrum, ForgeRock, and IBM Operational Decision Manager). The core eligibility application further integrates with other COTS applications (e.g., Adobe Experience Manager and AWS Connect) and custom applications (e.g., OCAT, Child Care Portal, and BenefitsCal).
2. **Interfaces with at least five external systems, at least one of which is real-time:** The CalSAWS solution interfaces and exchanges with 50 external systems. BenefitsCal, CalHEERS, County Master Data Management (MDM), Lobby Monitors, the Online CalWORKS Appraisal Tool (OCAT), and Statewide Client Index all interface in real time.
3. **Is accessed by at least 1,000 users at multiple locations:** The CalSAWS solution is accessed by an average of 18,500 daily users across 125 locations. After the CalWIN counties are migrated, the number of CalSAWS users will be approximately 41,500.
4. **Has a contract value of at least \$10,000,000 dollars:** The CalSAWS contract value is \$1,425,495,842.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The CalSAWS core eligibility application includes a multi-tiered processing architecture, a presentation tier optimized for multiple user interface platforms (e.g., Google Chrome and Microsoft Edge), an application tier, and a data tier. Other components of the system run on other user interface platforms such as kiosks and tablets.

I-F1 EXPERIENCE DETAILS

Accenture has been performing infrastructure operations for CalSAWS since the beginning of the project in November 2012 when it was called LRS. Migration related activities and planning from an on-premises data center to cloud hosting began in January 2019. Cloud-based operational activities began on October 14, 2019 and are currently ongoing. These activities include network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring.

Cloud-based operations

Accenture performs all cloud-based operations and was the prime contractor responsible for the cloud migration. This project involved the design, build, migration, and operation of the secure CalSAWS cloud. During the Design phase, we verified the AWS cloud was viable for the LRS platform for long-term use powering the statewide CalSAWS application. Transparency and widespread communication across all stakeholders were critical components during the assessment phase of the project. Accenture performed a proof of concept to assess potential capacity bottlenecks and confirmed that the AWS cloud support migration to cloud without significant changes. Accenture built a scalable and secure infrastructure for the system, migrated the primary 10-terabyte database and numerous ancillary databases, and migrated the existing 15,000+ county users to the new cloud-hosted architecture. With the migration complete, we now proactively manage all systems ensuring reliability and availability as part of our AWS cloud operating model. This accelerated process enabled LA County's legacy system to go live in the cloud a full month ahead of schedule.

Network engineering

CalSAWS uses a mixture of AWS cloud and on-premises network engineering solutions. We design and implement network configurations, provide network monitoring, and troubleshoot network performance issues. The network team engineered and maintained a network infrastructure designed to sustain high levels of availability for county and remote users. All network design changes align with state and federal policy. We proactively plan all new initiatives and expand the existing network infrastructure in line with the cloud migration. We also provide and implement solutions based on issues such as traffic congestion, infrastructure upgrades, and routine troubleshooting. Other activities include documenting solutions/blueprints for any network-related risks or issues, installing any hardware or software, creating back-ups for all systems, and monitoring the system performance. As a result, we have maintained a 99.8% uptime success rate with minimum impact to availability.

Cybersecurity vulnerability mitigations

We have put the Prevention-Detection and Correction framework in place at CalSAWS and created a significant reduction in cybersecurity risk levels by conducting a vulnerability assessment using tools such as Retina, QualysGuard, and Nmap covering servers and networking devices. We drive a balanced approach to cybersecurity that responds to potential risks from cybercrime/bad actors to prevent network breaches, data loss, and all immediate and future security/cybercrimes in the cloud and on-premises environments. We work proactively to identify potential risks and put mitigating solutions into place to prevent ecosystem breaches. We maintain a framework of risk management, controls, policies, processes, and metrics that are connected via a set of channels across the organization for setting expectations, measuring outcomes, and enacting change. We establish top-down accountability for owning, prioritizing, and protecting critical assets in an information-centric approach. We ensure the latest security practices are deployed consistently, have line of sight to people and security related processes and technology, and verify accountability structures drive the organization to continuously improve our security posture.

Capacity planning

Our operating model has a robust capacity planning process. The team consistently monitors demand and available resource levels where resource levels can easily be scaled up or down depending on demand. During the pandemic, we were able to rapidly adjust the number of resources needed based on an increase in the need for additional workload. For capacity planning at CalSAWS, we facilitate the collection of performance and capacity data of configuration items (CI). Capacity planning also includes monitoring, measuring, analyzing the performance of resources, and establishing capacity baselines, which profiles the use of resources and establishes an understanding of resource demand. Our planning efforts help us to accurately access the volume of resources to enable forecasting and planning across the environment.

Performance testing

Performance tests simulate peak load in a production-like performance environment by executing the most frequently used transactions. The workload mix at CalSAWS includes 37 critical business processes to replicate the online load. We select the critical business processes based on high frequency transactions and business criticality. The performance testing measurement validates the performance readiness of the release for deployment. The performance testing comprises the following tests: load, endurance, and stress test—all to identify the breaking point of the system under extreme load and determine the stability of the system. We analyze and report the test results. The server response times for each performance category are compared against application SLAs and the server metrics are captured. High response time or resource utilization scenarios are analyzed, and corrective actions are taken accordingly.

Performance monitoring

Monitoring and alerting are ongoing 24/7/365 activities performed using various monitoring tools including SolarWinds, Oracle Enterprise Manager (OEM), CloudWatch, and Dynatrace. These activities are achieved via automation and onsite staffing to confirm uninterrupted availability of the CalSAWS cloud-based infrastructure and application. These tools provide the ability to track specific events, infrastructure availability, and defined system thresholds. They include report-generating information such as availability, resource utilization, and other statistics.

The Operations Center monitors critical network devices, such as edge routers, firewalls, and core switches, as well as servers themselves. Operations Center personnel also monitor cybersecurity disruptions for possible intrusion and hacking attempts. In case of loss of connectivity to any network device, Operations Center personnel immediately prioritize the event based upon criticality of the device in question and notify CalSAWS network engineering or server administration personnel. All events are logged, and in the event of malicious activity, escalated to an incident. The incident response process includes description of minor and major incident processes, incident criteria, service level agreements, and other related information.

When predefined operational thresholds are surpassed or component failures are detected, monitoring tools automatically generate alerts to notify the Operations Center analyst. Once the alert is received, Operation Center staff members perform a high-level analysis to determine the severity. After determining the severity, the Operations Center analyst will notify the Level 3 Tech Team to investigate. The Tech team then marshals resources to resolve the problem. Depending on the severity of the issue,

a member of the Tech team informs members of the Consortium Tech team and/or other Consortium members. The Batch Operation team monitors file transfers between the CalSAWS system and county systems.

Project #4	Contact #4
Company Name: U.S. Department of Education, Office of Federal Student Aid	Contact Name: [REDACTED]
Project Name: Common Origination and Disbursement (COD) System Re-Architecture & AWS GovCloud Migration	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) Original COD contract March, 1, 2006 through September, 30, 2015 Current TIVOD/COD contract March, 1, 2015 through January, 31, 2025	Address: [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 227 months	Phone Number: [REDACTED]
Contract Amount: \$1,391,853,258	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture possesses four years and two months of experience performing cloud-based operational activities including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring on the Common Origination and Disbursement (COD) system that meets the definition of a large and complex IT system. Cloud-based operational activities began in 2018 and are currently ongoing through January 2025. Therefore, our experience on COD alone exceeds the requirement as one of the two projects needed for F1.</p> <p>PROJECT DESCRIPTION</p> <p>Common Origination and Disbursement (COD) is the U.S. Department of Education's Office of Federal Student Aid's (FSA) suite of applications to determine eligibility for federal, post-secondary financial aid. Launched in 2003 as a mainframe-based solution, the system processes approximately 30 million award originations and approximately 60 million disbursements, totaling nearly \$145 billion in aid annually. To support this financial aid processing, COD includes three websites that provide online services to financial aid recipients and their families, staff at post-secondary institutions, and thousands of FSA employees. Over 110,000 users</p>	

from a variety of locations, access these websites. The system has 390 active FSA (internal) users. To enable cost savings, improve agility, and enhance the security posture, Accenture was hired as the prime contractor to modernize COD by re-architecting it to run on a fully automated, modern technology stack and host it on a FedRAMP authorized cloud service provider.

Technical solution and services delivered

The hosting transition occurred in 2015 to establish the DevSecOps platform vision of accommodating the change flexibility and pace expected by the contract. The resulting platform allowed a greater percentage of the available budget to be delivered directly to aid recipients, reducing administrative and operational costs for the federal aid programs, and more securely stored the information of its 83 million unique customers' PII. The realization of the updated platform provided the initial building blocks to enable the transition to AWS GovCloud in 2018. After the re-architecture, the platform evolved to include industry-leading, innovative technologies for development, operations, and execution architecture.

These changes accommodated the pace of growth, expansion, and maintenance from 40 to more than 80 applications. This effort established a fully automated and serverless compute architecture with a focus on DevOps enablement. The migration to AWS transitioned all core components within a single weekend. The platform which originally supported four test environments has since scaled to support more than 40 test environments. Following the successful transition, Accenture assumed website hosting responsibilities from a client-contracted third-party contractor for StudentLoans.gov and ATS (two public-facing websites), to complete annual transactions. Accenture also rebuilt ~50 school reports, ~400 client reports/queries, and internal operations reports and dashboards to utilize the new reporting data store.

Accenture's cloud-based operations activities included network and system engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring. Accenture has over 16 years of experience performing application maintenance, system modifications, batch processing, hardware and software management, data conversion, project management, and service desk activities at COD. Our service desk activities include Information Technology Infrastructure Library (ITIL) standards and framework, supporting Tiers 1, 2, and 3 service desks/help desks, security, maintenance, and interoperability, with services continuing through January 2025 under the current contract.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** COD is comprised of multiple integrated application components. Its multi-tiered architecture includes front-end applications optimized for a variety of user interface platforms. It integrates with Oracle Service Cloud and the CRM tool, a COTS product, and with AWS GovCloud.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The COD back-end data tier is designed to be highly fault-tolerant and interfaces and exchanges with many external systems including the following:
 - Credit check – real time interface to credit bureaus (Equifax and Transunion) to confirm eligibility for a Grad PLUS or Parent PLUS loan
 - National Student Loan Data System (NSLDS)
 - National Enterprise Data Management and Analytics Platform Services (EDMAPS) – data lake and Person Master Data Management (pMDM) system for all student loan information
 - StudentAid.gov
 - PartnerConnect.ed.gov
 - Personal Authentication Service (PAS)
 - e-App – system that manages eligibility for participation in Title IV student aid
3. **Is accessed by at least 1,000 users at multiple locations:** 110,000 website users access COD in multiple locations. It contains 83 million client records and is the largest student aid system in the country.
4. **Has a contract value of at least \$10,000,000 dollars:** The contract value through option year 5 (2025) is \$1,391,853,258.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The COD solution includes multi-tiered processing, including a customer-facing front-end optimized for multiple user interface platforms, such as tablets and mobile devices.

I-F1 EXPERIENCE DETAILS

Accenture has been the prime contractor performing infrastructure operations on the COD system since the beginning of the project in March 2006. Migration from an on-premises data center to the AWS GovCloud began in March 2015 and was concluded in October 2018. Cloud-based operational activities began in 2018. Our operational activities include:

- **Infrastructure Operations:** Incident/problem management, defect management, batch operations, documentation such as runbooks, integration with external partners, network engineering, capacity planning, performance testing, and performance monitoring
- **Service Desk:** Success implementing and operating a multi-tiered service desk; Accenture is responsible for COD Tier 1, Tier 2, and Tier 3 service desk

- **Security:** Patch management, vulnerability management, security monitoring, business continuity, disaster recovery, error handling, and security incident management

Cloud-based operations

With over three million lines of COBOL code and billions of data records stored across both DB2 and IMS databases, COD was burdensome to maintain and enhance, and relied on costly, outdated technologies. To allow a greater percentage of the available budget to be delivered directly to aid recipients, reducing administrative and operation costs for the federal aid programs was a government priority. Additionally, with 83 million unique customers, securing individuals' PII data was paramount. To enable cost savings, improve agility, and enhance the security posture, it was necessary to modernize COD by re-architecting it to run on a fully automated, modern technology stack and host it on a FedRAMP authorized cloud service provider. The hosting transition occurred to establish the DevSecOps platform vision of accommodating the change flexibility and pace expected by the contract.

The implementation of the re-architected design replaced three million lines of COBOL code into Java PL/SQL application code and simplified the environment. As a result, the new environment processes more efficiently and with less operational overhead. The COD data migration was designed and planned to move the 18 billion records from legacy IMS and DB2 databases into the target Oracle databases. Security control improvements, such as data redaction, were also designed and implemented. This effort included the establishment of a fully automated and containerized development architecture with a focus on DevOps enablement.

Accenture's DevOps approach emphasized consistent and controlled cloud and on-premises environment configuration management as a means of mitigating delivery risk with a complex set of applications and managing fast paced, overlapping release schedules. This was achieved through 100% automation for all system components, the use of Red Hat Ansible, and a highly flexible configuration management database (CMDB). Ansible, which is tightly integrated with the CMDB, manages container creation, environment creation/maintenance, software installation/configuration, application configuration, and application deployment. It is integrated with Jenkins, Maven, and Nexus to fully automate the continuous deployment pipeline. The continuous integration and deployment pipeline also made use of Datical to automate the deployment of database changes and the CMDB to deploy environment specific configuration items.

All network logs, including creation and usage of virtual private clouds, security groups, route tables, and firewall activities from both cloud-native and COTS products are aggregated and reported on using centralized Splunk and CloudWatch dashboards. Accenture also implemented networking configurations to allow secure third-party connections into specific on-premises and cloud environments for ATO and penetration/vulnerability testing purposes. The Perimeter Infrastructure, included in each tenant, provides integration with Verizon MTIPS (TIC), routing between tenants and application systems, and is backed by a robust security architecture including WAF, Firewall, VPN, and proxy nodes.

Network engineering

COD utilizes a mixture of AWS cloud and on-premises networking solutions. We engineer and maintain a network infrastructure designed to sustain high levels of availability and security. This infrastructure maintenance includes physical and virtual networks, network security, and high availability.

Applications are decomposed to container services that each serve different areas of functionality and can be scaled independently, in a similar posture to a traditional micro-service architecture model. The applications can be adapted to ingest key/value properties and configuration data in each pod/container to increase configurability and overall solution scalability. This enables us to quickly pivot to customer demand while also reducing our response time to operational concerns. Over time, smaller application bundles leverage this containerized architecture to build smaller and more targeted container workloads in a DevOps-centric operating model.

All network design changes align with federal policy. We collaborate with COD to plan new initiatives, expand the existing network infrastructure, implement solutions, and provide routine troubleshooting. We document solutions and blueprints for any network-related risks or issues, install hardware or software, create back-ups for all systems, and monitor the system performance. We have maintained a 99.8% uptime success rate with minimum impact to availability.

During a particular deployment, the Accenture team held extensive implementation planning meetings to define a 96-hour window for a 900-task deployment plan. Where possible, individual portions of the deployment plan were executed in “dry run” exercises in temporary environments built on the production infrastructure. This approach allowed the team to refine the plan and ensure a tightly managed deployment where every minute of the 96 hours was effectively used and accounted for. Unsurprisingly, the deployment was very predictable. The implementation ran on schedule and the effort culminated in the successful deployment of the new COD2.0 processing platform.

Cybersecurity vulnerability mitigations

We use a balanced cybersecurity approach to detect potential risks from cybercrime/bad actors—preventing network breaches, data losses, and immediate and future security/cyber-crimes. We proactively identify potential risks and employ mitigation strategies to prevent ecosystem breaches. Accenture maintains a framework of risk management, processes, policies, controls, and metrics that are integrated across the organization to set expectations, measure outcomes, and enact change. We establish top-down accountability for owning, prioritizing, and protecting critical assets in an information-centric approach. We validate that the latest security practices are consistently deployed, with a line of sight to people and security related processes and technology. We verify that the accountability structures drive the organization to continuously improve our security posture.

COD uses a monthly patching process using AWS Systems Manager Agent (SSM Agent) to identify and patch servers across its infrastructures to the same patch level and package set. This enables the team to validate that all patches are tested prior to deployment into production. Additionally, the patch cycle can be expedited and run in a one-off basis to address any issues. The infrastructure for COD is scanned daily for any new vulnerabilities.

COD implements security throughout the system focusing on a "least privileges possible" model for individuals and systems, network access management, data encryption, and rigorous patch and vulnerability management that restricts users to only access systems necessary to complete their required functions. COD develops access roles, policies, and procedures (including AWS Identity and Access Management (IAM)) to ensure proper review and approval are completed for all access requests to COD systems. COD has deployed a centralized user credential and privilege system using a custom application and open-source Lightweight Directory Access Protocol (OpenLDAP) implementation, which is integrated with each system component. Additionally, privileged actions within COD are logged and monitored through Centrify and host-based log forwarding to Splunk for review and analysis by the virtual security operations center (vSOC) which provides 24/7 SOC analysts to monitor COD security events.

Accenture implemented automations to manage the infrastructure using AWS. Previously, the infrastructure was being manually maintained in the data centers, which included the network, compute, storages, and all inter-dependent and environment component integrations. In addition, the DevSecOp tools and reference architecture needed to expand to establish virtual firewall devices, which included a web application firewall, patch management, and ongoing infrastructure and application scanning.

Capacity planning

Capacity planning includes monitoring, measuring, resource performance analysis, baseline creation, and provides an understanding of resource utilization and demand. Our planning efforts help to access the volumes of resources, enabling environment forecasting. Capacity planning is organized into multiple sprints within program increments. These are structured by tickets/requests that flow through our Architecture Review Board (ARB) or Technical Review Board (TRB) and then slated to the appropriate sprint.

Application and system business metrics are collected and aggregated to inform scalability needs for upcoming weeks and months. Capacity is accounted for and scaled ahead of time with automated alerting driven by Splunk and AppDynamics, enabling operations teams to react ahead of impact. We use the following tools to drive these processes:

- Node health (used when Garbage Collection Time is too high, CPU utilization is too high, JVM Garbage Collection Time is too high, JVM Heap utilization is too high, or memory utilization is too high)
- Business transaction performance alerts (used to show response times, JVM error rate, JVM average response times, transaction call rates, and transaction stall counts)

Integration with the AWS cloud application programming interface (API) for infrastructure management has resulted in the following successes:

- We can destroy and recreate every component, including the networking.
- We have the capacity to establish isolation between security zones.
- We can build everything through automation.

- We can manage our operations team with Ansible.

Accenture selected the AWS API to maintain a consistent approach to automation by leveraging Ansible. Enhancements to the Ansible modules for the AWS API accommodated the platform integration needs because they allowed for a single control point for all architecture management. Moving to AWS allowed us to streamline our APIs across the system, which offered better integration with other partners and promoted industry-standard best practices.

Performance testing

Our performance test approach focused on baselining the performance of the legacy system, mapping all legacy applications to their re-architected counterparts, and building an industrialized performance testing capability for the new solution. Using a wide variety of tools—including RadView WebLoad, Oracle OEM, Oracle AWR, and AppDynamics—Accenture executed extensive tests both in isolation and with production-level volumes across the full suite of applications. The performance test process identified problematic areas and allowed the team to remediate those issues prior to deployment. The new solution exceeded performance targets and demonstrated high levels of stability and efficiency that assured a successful production deployment.

We provide an integrated operations and performance testing capability for COD. Testing is conducted prior to the implementation of any system change. Our technical architecture team provides input to the overall system design to maximize system performance and maintainability, and leverages production-like test data to effectively mimic peak data processing scenarios. Our performance testing process of leveraging production-like test data and mimicking peak data processing scenarios ensures that we can successfully meet or exceed performance measures for COD system availability in production.

Performance monitoring

Monitoring and alerting are ongoing 24/7/365 activities performed using various monitoring tools. These activities are achieved using automation and onsite staffing to confirm uninterrupted availability of the COD cloud infrastructure. Performance monitoring tools like Splunk and AppDynamics catch issues before system users become aware of an issue. These tools provide the ability to track specific events, infrastructure availability, and defined system thresholds. They include report-generating information such as availability, resource utilization, and other statistics. The Operations Center monitors critical network devices such as edge routers, firewalls, core switches, and the servers. Operations Center personnel also monitor for possible intrusion and hacking attempts. In the event of a loss of connectivity to a network device, Operations Center personnel prioritize the event based upon criticality of the threatened device and notify the appropriate personnel. All events are logged, and in the case of malicious activity, escalated to an incident. When predefined operational thresholds are surpassed or component failures are detected, monitoring tools automatically generate alerts to notify the Operations Center Analyst. Once the alert is received, Operation Center staff members will perform a high-level analysis to determine the alert severity. After determining the severity, the Operation Center Analyst will notify the Level 3 Tech Team to investigate, whereupon they will coordinate resources to resolve the problem.

Project #5	Contact #5
Company Name: State of Texas	Contact Name: [REDACTED]
Project Name: Texas Centralized Accounting and Payroll/Personnel System (CAPPS) Managed Services	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) December, 30, 2014 through August, 31, 2024	Address: [REDACTED] [REDACTED]
Contract Duration (months): 116 months	Phone Number: [REDACTED]
Contract Amount: \$155,000,000	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture has eight years of prime contractor experience performing cloud-based operational activities on the Centralized Accounting and Payroll/Personnel System (CAPPS), a system that meets the definition of a large and complex IT system. Therefore, our experience on CAPPS exceeds the requirement for one of the two projects needed for F1.</p> <p>PROJECT DESCRIPTION</p> <p>CAPPS is the enterprise resource planning (ERP) solution for the State of Texas. The state, under the direction and leadership of the Texas Comptroller of Public Accounts (CPA), is facilitating a multi-year effort to expand the CAPPS Finance and HR systems to all Texas state agencies. Before CAPPS, each state agency had its own ERP. The objective of CAPPS is to provide state agencies with a single system to enhance the effectiveness of operations and encourage agencies to migrate from their legacy systems to CAPPS. Another aspect of the strategy is to allow certain agencies to develop their own systems, referred to as a hub, and interface to CAPPS. The resulting, more efficient system eliminated the duplicated effort and complexity created from having hundreds of systems in the state.</p> <p>Additionally, Texas CPA is the first state government client to migrate to the Oracle Cloud Infrastructure (OCI). We completed the migration to the cloud project in seven months. The migration scope included provisioning three availability domains across two regions, 83 environments, 67 virtual servers, and three Exadata Cloud Service components. The go-live was smooth, with minimal post-go-live issues.</p>	

Technical solution and services delivered

The TX CPA CAPPs project operates as a high-performing and complex HCM and FIN PeopleSoft implementation. As a prime contractor, Accenture performs application maintenance, system modifications, cloud-based operations, network and system engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, performance monitoring, and batch processing. Accenture currently supports CPA and various state agencies to sustain the CAPPs application, continue to enhance capabilities, onboard additional state agencies to CAPPs FIN and HCM, and add additional functionality/new modules to the system. Accenture also leads all project management functions and project reporting (daily, weekly, monthly, and annually).

Texas CPA has rolled out seven successful waves for FIN and HCM towers for 100 agencies. The project also originally included a transition in 2015. Accenture continues to provide 24/7 operations/steady-state support of this complex system that includes support of numerous legacy systems and processes more than \$90 billion in state spending, representing 92% of all spend in Texas state agencies. The TX CPA will continue to deploy to the remaining agencies and non-core modules to additional agencies through 2024 under the current contract that is valued at \$155 million.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CAPPs solution integrates with several applications including PeopleSoft, Control-M, and Phire, all of which are COTS.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The CAPPs solution interfaces with 105 external systems including two external state web services (the state recruitment website and the website to validate Social Security numbers in the Texas retirement system) in real time.
3. **Is accessed by at least 1,000 users at multiple locations:** The system supports 113,000 employees in multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The CAPPs contract value is \$155 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** Our PeopleSoft-based solution uses multi-tiered processing, including a user-facing front-end and adapts to multiple user interface platforms.

I-F1 EXPERIENCE DETAILS

At CAPPs, Accenture has eight years of prime contractor experience performing infrastructure and cloud-based operational activities. These activities include network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring. We began planning the migration from an on-premises data center to private cloud hosting at the start of the project in December 2014. The migration to the cloud project was completed after eight months in August 2015. The migration scope included a fault-tolerant multi-location private cloud supported by a virtualized, software-defined infrastructure. In April 2019, Texas CPA became the first state government ERP project to migrate to OCI. The migration

scope included provisioning three availability domains across two regions, 83 environments, 67 virtual servers, and three Exadata Cloud Service components. The CAPPs project is ongoing through August 2024.

Cloud-based operations

This project involved migration to cloud. We verified that Oracle Public Cloud would be a viable platform for long-term use powering CAPPs. Accenture performed a proof of concept to assess potential capacity bottlenecks and confirmed that the cloud migration would not require significant changes. We designed and implemented a scalable and secure infrastructure for the system, migrated the primary database and numerous ancillary databases, and migrated 64,000 existing users to the new cloud-hosted architecture.

Accenture's solution includes implementing, maintaining, and operating the following technologies:

- **Oracle-engineered systems (like Exadata and private cloud appliance):** We currently use Exadata Cloud Service as our application database. We have 20-plus container databases (CDBs) and more than 70 pluggable databases (PDBs) across three Exadata quarter racks, two 30 Oracle central processing units (OCPU), and one 42 OCPU.
- **Oracle database and middleware products:** We use Tuxedo and WebLogic as middleware products. Tuxedo is our application server middleware, and WebLogic is our web server. We use Oracle Database 19c hosted on Exadata Cloud Service X8M for our databases.
- **Windows servers:** We have 25 Windows servers using the 2016 and 2019 versions to support our application in several different ways including performance testing, security and monitoring tools, remote desktop enablement, and PeopleSoft Update Manager.
- **BMC Control-M:** We use BMC Control-M to perform complex batch application support, job scheduling, job creation, scripting, and administration.

Linux patching is completed through Spacewalk software that we have installed on a virtual machine (VM). Windows patching is completed through Windows Server Update Services (WSUS). Windows and Linux patching is planned monthly with non-production and production completed in separate change windows. Windows version upgrades are completed in the cloud by creating a new VM on the newer operating system version and reimplementing the applications from the old server. Linux upgrades are completed through Spacewalk. Monitor alerting is done through Oracle Enterprise Manager (OEM), PeopleSoft 360, and custom scripts. The alerts are a combination of ServiceNow incidents and emails. OEM is installed on a cloud VM, PeopleSoft 360 is on Splunk, and custom scripts run through the Control-M batch scheduler or CRON. The Control-M batch scheduler is installed on a cloud VM with agents installed on other VMs.

Accenture continues to provide 24/7 operations/steady-state support of this complex system that includes support of numerous legacy systems, over 113,000 state employees, and will process more than \$90 billion in state spending, representing 92% of all spend in Texas state agencies. The go-live was smooth, with minimal post-go-live issues. Additionally, the TX CPA CAPPs project

has led to other states—including Virginia's ERP and Kansas's integrated eligibility system—migrating to OCI. Other states are looking closely at moving to OCI. The project was recognized with several external awards and speaking engagements.

Network engineering

CAPPS features a mixture of OCI and on-premises networking solutions. We engineered and maintained a network infrastructure designed to sustain high levels of availability and security. This infrastructure maintenance includes configuring virtual networks, network security, and high availability. All network design changes align with applicable state and federal policies. We plan all-new initiatives and expand the existing network infrastructure in line with the migration to provide and implement solutions based on issues such as traffic congestion, infrastructure upgrades, and routine troubleshooting. We also document solutions/blueprints for any network-related risks or issues, install any hardware or software, create backups for all systems, and monitor the system performance. We maintain a 99.8% uptime success rate with minimum impact to availability.

Cybersecurity vulnerability mitigations

We drive a balanced approach to cybersecurity for potential risks from cybercrime/bad actors to prevent network breach, data loss, and all immediate and future security/cyber-crimes. We proactively identify potential risks, put mitigating solutions into place to prevent ecosystem breaches, and maintain a framework of risk management, controls, policies, processes, and metrics that are connected through a set of channels across the organization for setting expectations, measuring outcomes, and enacting change. We also establish top-down accountability for owning, prioritizing, and protecting critical assets in an information-centric approach. We make sure the latest security practices are deployed consistently and have line of sight to people and security-related processes and technology. We verify the accountability structures drive the organization to continuously improve our security posture and put the Prevention—Detection and Correction framework in place. This resulted in a significant reduction in cybersecurity risk level by conducting a vulnerability assessment using tools for servers and networking devices.

Capacity planning

Our role in capacity planning includes monitoring, measuring, and analyzing the performance of cloud and on-premises resources. We establish capacity baselines that profile the use of resources and create an understanding of resource demand. The performance of environments is the basis for forecasting and planning. The team classifies capacity needs into production and non-production based on business needs. We monitor operational capacity and engage in planning to determine the budgeting and scaling requirements. In the capacity management process for CAPPS, we collect performance and capacity data for configuration items, changes, enhancements, etc. and then monitor, measure, and analyze the capacity baseline so we can forecast and plan for capacity requirements in the future. We also participate in release planning, configuring for, and deploying additional resources.

Performance testing

The performance test simulates peak load on the infrastructure in a production-like performance environment by executing the most frequently used transactions. The workload mix includes critical business processes to replicate the online load, which we

select based on high-frequency transactions and business criticality. To validate the performance readiness of the release for deployment, we use performance tests including the atomic test (single user, single transaction), 100% peak test, and 200% peak test. These help us identify the breaking point of the system under extreme load and determine the stability of the system. We analyze and report the test results and then compare the server response times for each performance category against application SLAs, capturing the server metrics. We analyze high response time or resource utilization scenarios and take corrective actions as needed. The project uses Load Runner Cloud for load and performance testing. Performance test runs are completed as a part of the yearly deployment. Several tests will be run with an increased number of user sessions in a specific period, and the performance outcomes from the recorded graphs are analyzed for assessment of any concerning impact.

Performance monitoring

Monitoring and alerting are ongoing 24/7/365 activities performed using various monitoring tools including OEM, PeopleSoft 360, and custom scripts. These activities are achieved using automation and onsite staffing to confirm uninterrupted availability of the CAPPS infrastructure and application. These tools provide the ability to track specific events, infrastructure availability, and defined system thresholds. They include report-generating information such as availability, resource utilization, and other statistics.

Minimum Experience I-F2

Prime Contractor experience with the transition of one (1) cloud-based system from one company to another involving a large and complex IT System. The transition component of the Project must have completed within the last five (5) years.

Project #1	Contact #1
Company Name: State of Arizona, Arizona Health Care Cost Containment System (AHCCCS)	Contact Name: [REDACTED]
Project Name: Health-e-Arizona Plus (HEAplus) M&O	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) October, 1, 2020 through September, 30, 2024	Address: [REDACTED]
Contract Duration (months): 48 months	Phone Number: [REDACTED]
Contract Amount: \$121,000,000	Email: [REDACTED]
Describe the services provided:	

EXPERIENCE SUMMARY

Accenture has prime contractor experience transitioning one cloud-based system from one company to another for HEAplus, a system which meets the requirements of a large and complex IT System. The transition was completed in May 2021, and therefore **meets the requirement** stated in F2.

PROJECT DESCRIPTION

Health-e-Arizona Plus (HEAplus) is the State of Arizona's \$14 billion eligibility determination and case management system, administering public assistance benefits for the Arizona Health Care Cost Containment System (AHCCCS) and the Arizona Department of Economic Security (ADES) agency. HEAplus provides a web-based portal for consumers, eligibility workers, and community assistors, and supports eligibility determinations and ongoing case management for benefit programs including Medicaid, Children's Health Insurance Program (CHIP) (known as KidsCare in Arizona), Medicare Savings Program (MSP), and the Arizona Long-Term Care System (ALTCs). HEAplus takes the application for SNAP and TANF, and interfaces with the DES mainframe system for eligibility determination and benefit calculation.

Technical solution

HEAplus is a cloud-based eligibility system with a public-facing portal used by Arizona residents, community assistors, and state employees. The application uses a multi-tier architecture with .NET front end and SQL Server database. HEAplus collaborates with county departments and non-county medical assistance (MA) sites to administer MA programs throughout the State of Arizona, as well as the SNAP and TANF programs. The objective of the project is to offer the most accurate, credible, and real-time eligibility determinations for the State, which serves over 3,900 internal state workers and over 2.43 million Arizonans (external users), 1.75 million of whom use the portal which includes multiple user groups from the worker and self-service portals. The system processes 22,250 daily eligibility cases.

Services delivered

In 2020, the AHCCCS, the Medicaid agency responsible for HEAplus, awarded Accenture an initial five-year Maintenance & Operations (M&O) contract to maintain the system by introducing transparency and efficiency to the overall system operations. The contract includes application maintenance, system modifications, hardware, software, project management, security, and enhancements of all system components. Starting in October 2020, Accenture, as the prime contractor, worked with the incumbent to transition the support of the infrastructure as a service (IaaS) footprint for the State of Arizona, which had previously migrated to Microsoft Azure Cloud. Cloud-based operational activities include system and network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing, and performance monitoring, and batch processing—which are ongoing through September of 2024.

After the successful transition in May 2021, Accenture shifted focus to providing innovative and comprehensive services to maintain the HEAplus system in Azure Cloud—improving scalability and flexibility for business and policy initiatives. The contract

supports a multi-contractor design in collaboration with AHCCCS, ADES, the Department of Correction, Accenture, Exela, IMI, Valor, Office Max, and Microsoft.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** HEAplus interfaces with numerous SaaS services, COTS, applications, and interface partners. The COTS products extensively used in HEAplus are Elastic Search, Google Analytics, and Fortify.
2. **Interfaces with at least five external systems, at least one of which is real-time:** HEAplus interfaces with at least five external systems including CMS Hub (real-time interface with CMS Hub for Citizenship, VLP, verify current income), SSA (for real-time SOLQi call), Equifax (real-time and batch for Wages income), Federally Facilitated Market Place (FFM) for Account transfers (real-time), ADOT (real-time interface with Arizona Department of Transportation for residency verification), eDRS (real-time federal interface on Disqualified Recipient System), and SAVE (real-time federal interface on Systematic Alien Verification for Entitlements). All seven interfaces are real-time.
3. **Is accessed by at least 1,000 users at multiple locations:** Over 1.75 million Arizona residents at multiple location accessed the HEAplus solution, including multiple user groups from the worker and self-service portals.
4. **Has a contract value of at least \$10,000,000 dollars:** The HEAplus contract value is \$121 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The application uses a multi-tier architecture with .Net front end, SQL Server database, and interfaces with numerous SaaS services, COTS, applications, and interface partners. It is optimized for multiple user interface platforms, such as tablets and mobile devices.

I-F2 EXPERIENCE DETAILS

As the prime contractor, Accenture began working with the incumbent to transition the support of the infrastructure as a service (IaaS) footprint for the State of Arizona at project launch in October 2020. Our responsibilities included transitioning-in and taking over maintenance and operations from the incumbent contractor under challenging circumstances. With very little technical or functional documentation to work with, and unable to access the existing codebase and database due to an uncooperative outgoing contractor, Accenture was limited to minimal knowledge transfer meetings per week with the incumbent. We created a plan uniquely built with and for Arizona using our holistic Transition-In methodology and incorporating our Program, People, Process, Technology, and Productivity approach as guideposts.

Some specific items included:

- Transition Planning and development of the master schedule
- Development and execution of the transition work schedule

- Production and execution of the meeting calendar, cadence, knowledge transition, and status reporting
- Migration and service integrated activity plan
- Development of the Transition-In Master Schedule
- Staffing and resource onboarding plan
- Service management process, SLAs, and reporting
- Connectivity setup, including access assessment and enablement
- Process enhancements and automation
- Transition readiness reviews and approvals
- Test and validation schedule

Our limited knowledge transfer (KT) from the incumbent included documentation of the existing workstreams including eligibility, eligibility support, eligibility appeals, exemptions, enrollment, applications, notices, issuer payments, and plan review and certification. To complete the knowledge gathering phase, Accenture's Infrastructure team created documentation based on the information that was gathered and knowledge of similar environments. Documentation included cloud functions, components, and infrastructure for both production and non-production environments. Accenture used our proprietary tools to gather the necessary infrastructure configurations as part of the documentation phase. Accenture worked in close collaboration with AHCCCS leadership and staff according to the schedule and to minimize operational risk to AHCCCS.

AHCCCS also requested Accenture build the Operational Readiness Test (ORT) environment, a task typically owned by the incumbent. Although no usable scripts were provided, Accenture's Infrastructure team seamlessly built the environment and executed ORT. This exceptional effort led AHCCCS to request Accenture complete cutover activities earlier than planned and assume maintenance and operations as soon as possible. Our team met the new deadline and received praise from multiple stakeholders for the smooth transition.

Outcomes delivered:

- Executed Operational Readiness Test successfully, with over 50 scenarios
- Ensured all IaaS components were exceeding agreed upon SLAs and KPIs
- Configured all necessary software, tools, and licenses, and achieved client acceptance of all transition deliverables, enabling a three-week accelerated cutover
- Performed cutover successfully without outages, disruptions, or major issues

Within eight months and ahead of schedule, transition from the incumbent was completed in May 2021. Following the successful transition, Accenture now provides comprehensive services to maintain the HEAplus system in Azure Cloud with greater scalability,

transparency, and flexibility for business and policy initiatives. Accenture services and support will continue through September 30, 2024.

As a result of the transition, Accenture became responsible for the ongoing maintenance of the following:

- Ensuring all IaaS components exceed agreed upon SLA's and KPI's (service levels)
- Monitoring of the cloud from a performance and cost perspective, and performing scale up and down activities as necessitated by the load on the platform
- Working with state to rectify licensing issues during transition and implementing a program to verify that licenses, software, service contracts, and certificates were procured in the state's name
- Validating policy and security standards are followed and appropriately reported
- Performing system alert and monitoring gap analysis

Analysis was based on our experience and lessons learned in maintaining numerous integrated eligibility systems of similar size and scope. The customized HEAplus report identified several gaps in alert conditions, ranging from firewall monitoring to system security alerts. Accenture reviewed the results with the Arizona team and followed up with a significant effort to close the discovered gaps.

Minimum Experience I-F3

Prime Contractor experience providing service desk activities on two (2) Projects of at least 12 months in duration each involving large and complex IT systems using Information Technology Infrastructure Library (ITIL) standards and framework. Service Desk experience must include supporting Tiers 1 and 2 service desks/help desks, security, maintenance and interoperability. Each of the two (2) Projects must have been completed or ongoing within the last five (5) years.

Project #1	Contact #1
Company Name: State of Ohio, Department of Administrative Services (DAS)	Contact Name: [REDACTED]
Project Name: Ohio Benefits	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) February, 20, 2013 through June, 30, 2023	Address: [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 124 months	Phone Number: [REDACTED]

Contract Amount: \$530,000,000	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture has over nine years of experience performing service/help desk activities using Information Technology Infrastructure Library (ITIL) standards and framework at Ohio Benefits, a system that meets the definition of a large and complex IT system. Service desk activities are currently ongoing through June 30, 2023, therefore, our experience at Ohio Benefits exceeds the requirement as one of two projects needed for F3.</p> <p>PROJECT DESCRIPTION</p> <p>The Ohio Benefits program is a mature enterprise system that streamlines health and human services program delivery through standardized business processes which improve client outcomes. Ohio Benefits was initiated in 2012 to transform Ohio's enterprise integrated eligibility and health and human services system. It was designed to replace the 30-year-old Client Registry Information System, Enhanced (CRIS-E). The primary function of CRIS-E was benefit eligibility determination for beneficiaries of the Ohio Department of Job and Family Services (ODJFS) and Ohio Department of Medicaid (ODM) programs.</p> <p>Ohio Benefits first went live in October 2013, and currently supports eligibility determination and benefit distribution for the State's Medicaid (including CHIP), SNAP (including P-EBT), Cash (including Temporary Assistance for Needy Families (TANF) and Refugee Cash Assistance), and Child Care programs. Ohio Benefits supports over three million residents and is used by over 10,000 county users across multiple locations in 88 counties.</p> <p>Technical solution</p> <p>Ohio Benefits integrates multiple COTS products including the Accenture Public Service Platform, IBM Cognos, Informatica Master Data Management, Adobe Experience Manager, and Tableau. Accenture implemented and supported Ohio Benefits with an innovative and scalable infrastructure designed for high availability, stability, and performance using Oracle's Private Cloud platform. Accenture implemented Oracle Linux virtual servers, Oracle databases, a series of Oracle Middleware products, and other software on this platform. Over time, Accenture implemented five key portals for the program: Citizen Self-Service Portal, Worker Portal, Provider Portal, Presumptive Eligibility/Deemed Newborn Portal, and Business Intelligence (BI) Portal.</p> <p>The system supports integration with 47 state, agency, and other external interface partners and systems, including approximately 85 data exchanges (both real-time web services and file-based transfers). Interface partners include federal agencies such as the SSA, CMS, DHS, and IRS. Seven million real-time transactions are exchanged each month with various interface partners.</p> <p>Benefit issuance data is transmitted to SNAP and Cash issuance contractors to deliver more than \$2.25 billion in annual SNAP payments, more than \$180 million in annual Cash payments, and over \$1 billion in P-EBT benefits since the beginning of the</p>	

COVID-19 public health emergency. Real-time data is exchanged with the State's MMIS system, MITs, to support Medicaid service delivery for more than 3 million Ohioans. The system is architected for multi-tiered processing, including a user-facing front end designed to adapt to multiple user interface platforms (e.g., laptops, phones, and tablets).

Services delivered

In February 2013, Accenture was awarded the contract for Design, Development, and Implementation (DDI) for implementing the Medicaid, SNAP, TANF, and Child Care programs into Ohio Benefits and subsequent M&O services to support the administration of programs in the production environment. Accenture has served as the prime contractor for this project since inception, and the current contract ends in June 2023.

Accenture's infrastructure support for Ohio Benefits includes operations, performance testing, performance monitoring, security, network engineering, cybersecurity vulnerability testing and mitigation, capacity planning, and managing hardware and software. Accenture's application M&O support includes application maintenance, system modifications, system engineering, capacity planning, performance testing, performance monitoring, batch processing, data conversion, and project management.

Accenture also supports the Ohio Benefits solution via a multi-tier service desk (tiers 1, 2, and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework. Accenture is responsible for all phases of the enhancement software development lifecycle, including Analysis, Design, Development (Build) and Test, Deployment, and Post-Deployment.

Accenture partners with multiple contractors on the program, including Deloitte for organizational change management services, Northwoods for electronic document management services, and Cincinnati Bell (CBTS) for computer telephony integration and interactive voice response services.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** Ohio Benefits is based on multiple COTS products including the Accenture Public Service Platform, IBM Cognos, Informatica Master Data Management, Adobe Experience Manager, and Tableau. Ohio Benefits runs on dedicated infrastructure leveraging Oracle's private-cloud platform: Oracle Exadata systems, Oracle Private Cloud Appliances, and Oracle ZFS storage, along with other third-party hardware security and operations components such as Micro Focus ArcSight and Veritas NetBackup.
2. **Interfaces with at least five external systems, at least one of which is real-time:** Ohio Benefits implements 85+ interfaces across 47 partners, including both State and Federal partners, such as the IRS, SSA, Accuity (Asset Verification – real-time), Central Print, Ohio Department of Health and Human Services (public assistance reporting), and Ohio Department of Developmental Disabilities (waiver eligibility information), among other partners. Batch and real-time interfaces are implemented leveraging Axway API gateway.

3. **Is accessed by at least 1,000 users at multiple locations:** Ohio Benefits supports over three million residents, and over 120,000 users access it across multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The Ohio Benefits contract value is over \$530 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** Ohio Benefits includes multi-tiered processing with a mobile-friendly, customer-facing front end for Self Service Portal (SSP) for Ohio residents.

I-F3 EXPERIENCE DETAILS

Accenture has been performing service desk activities for Ohio Benefits since the beginning of the project in February 2013. These activities include using ITIL standards and framework, supporting Tiers 1, 2, and 3 support, security, maintenance, and interoperability.

Overview of service desk

Accenture provides Level 1 Service Desk, including logging incidents, assisting Ohio county workers for known issues, and referring incidents. We also provide Level 2 Service Desk (including Functional SMEs), including incident and problem triage, technical execution, document workarounds, and resolution of incidents. In addition, we provide Level 3 Service Desk (defect fix) which includes problem triage support, delivering warranty defect fixes, compliance, and applying technical workarounds.

Using ITIL standards and framework

At Ohio Benefits, we employ the ITIL standards and framework. This provides a cohesive set of leading practices, drawn from the public and private sectors internationally as a widely accepted approach to IT service management. Accenture Delivery Methods has incorporated ITIL best practices and terminology, with ITIL as the foundation for our Infrastructure Consulting methods. Accenture has thousands of individuals trained in ITIL and has been actively involved with the IT Service Management Forum, the ITIL user group, as well as the Office of Government Commerce (OGC) as the owner of ITIL. Alongside Carnegie Mellon University, Accenture is a co-author of the Service Strategies book, one of the five volumes in ITIL v3.

ISO 20000 (previously published as BS15000) is an international standard for IT Service Management based on ITIL. While ISO 20000 defines the requirements for service providers to plan for and deliver managed services, it also represents an industry consensus to help prepare for audits against ISO 20000. Accenture has achieved the ISO 20000 certification in multiple locations. The use of ITIL on the Ohio account promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements.

Service desk experience, including supporting Tiers 1 and 2 service desks/help desks

At Ohio Benefits, we provide a fully operational service desk. It is based on a multi-tier service desk model and is organized into three tiers: Tier 1, 2 and 3. Each Tier of model works as follows:

- Tier 1 is the initial contact point for interactions with the Service Desk. Tier 1 will create cases for each interaction, triage, categorize the case, attempt to resolve and, if necessary, escalate to Tier 2 with the creation of a related Incident.
- Tier 2 will review the escalated Incident and attempt to resolve it. Upon resolution, the incident and related case(s) are all closed. For incidents that cannot be resolved by Tier 2, Tier 2 will escalate to Tier 3 for resolution.
- Tier 3 is staffed with our infrastructure, application development, production operations and technical subject matter experts. Tier 3 will create an incident ticket, assign to the appropriate expert for application fixes or workarounds. Upon resolution, the problem and related incident(s) and case(s) are closed.

The Ohio Benefits Service Desk handles ~3,000 incidents per month. Incidents are prioritized by criticality and addressed using the following standards:

- P1/Critical: Resolution <=4 hours; incident status provided every 15 minutes until resolution
- P2/High: Resolution <= 8 hours; incident status provided every 30 minutes until resolution
- P3/Medium: Resolution <= 5 business days; incident status provided every 24 hours until resolution

This service desk model shows that end-users are provided with the level of support needed to accelerate resolution.

Security

The service desk is alerted when security incidents are detected. The Security Operation Center (SOC) will receive a ticket/notification to investigate the incident of a potential breach. Once they have completed their investigation and remedy the security-related issue, they notify the service desk, and the ticket is closed. Examples of security related incidents include unusual behavior of privileged user accounts; unauthorized insiders trying to access servers and data; phishing anomalies in network traffic; excessive consumption of server memory; unauthorized changes in configuration and unexpected account lockouts and password changes. The service desk works in collaboration with the SOC to ensure all aspects of security are communicated and resolved across the ecosystem.

An information security program providing confidentiality, integrity, and availability is critical to Ohio Benefits. We handle and protect large amounts of personal and health information (PII/PHI) provided by users and State and Federal agencies. We follow multiple compliance frameworks and privacy requirements such as CMS MARS-E, HIPAA/HITECH, FISMA/NIST standards, ACA Privacy, and State security and privacy policies.

The Department of Administrative Services provides the policies that we must adhere to when designing, developing, implementing, and operating Ohio Benefits service desk and operations. These policies are based on National Institute of Standards and Technology (NIST) standards, the customized System Security Plan (SSP). The Chief Information Security Officer has oversight responsibilities that include the testing and validation of the contractor implementation of the NIST SP 800-53 security controls. In addition, the client security team performs audits periodically focused on technical vulnerabilities for the overall program and interconnected systems. This team also supports the independent third-party technical security audit performed on a regular basis.

The audits assess that:

- The implementation of each control is documented with evidence to prove compliance to the control.
- Technical systems properly implement the security control according to the Center for Internet Security (CIS) controls benchmark standard for the appropriate technology.
- The non-technical controls are properly implemented according to the processes documented in compliance with NIST CyberSecurity Framework, ISO27002, SOC2 and State security policies, standards, and control baselines.
- Any known deficiencies are properly documented with Plan of Actions and Milestones (POAMs) created to track their remediation.

A report will detail the results categorized by each NIST control family and provide the remediation for the security control according to the CIS benchmark.

Accenture provided several security services:

- Access Control, including regular access control audits of users provisioned to roles and permissions assigned to roles
- Specialized security role training for contractor and Subcontractor personnel employed in security roles
- Monitoring and alerting provided by a centralized Security Information and Event Monitoring system that is monitored 24/7, with ingestion from across Ohio Benefits components and resources
- Security assessment of all modifications, changes, and acquisitions for the system
- Regular auditing of System configurations and changes, to confirm an accurate accounting of all system components and proper execution of Change Management processes
- Security integration with contingency planning and disaster recovery activities and testing
- Operation and maintenance of identity management systems that provide authentication and authorization functions across Ohio Benefits and supporting infrastructure
- Security incident response, including a 24/7/365 response capability to address security incidents based on severity and impact to the confidentiality, integrity, and availability of the system

- Continuous security vulnerability scanning and remediation within required timeframes, including coordination with infrastructure and application release management activities

The Department of Administrative Services participates in the architectural standards Review Sessions to confirm accountability, transparency, responsiveness, inclusiveness, empowerment, and broad-based participation in the development of Secure Architectural Standards. They facilitate the approval process and adoption of standards.

Maintenance

The Ohio Benefits Self-Service (resident-facing) Portal is available and accessible 24 hours a day, 7 days a week, and 365 days a year except for scheduled downtime. The maintenance of the knowledge base has been architected to refresh periodically with the latest content library includes tutorials that guide the user step by step through how to use key software features and resolve simple errors they might encounter. The Worker Portal is online during day, and offline while batch processing is completed at night. The Ohio Benefits system is architected to be up when Ohio Benefits nightly batch is running. Service desk maintenance is comprised of identifying the improvements needed when it comes to people, process, and procedures. Maintenance is a continuous improvement process to ensure residents and workers have the latest information, policies, and features.

M&O services encompass the project and operational management of Ohio Benefits. Accenture provides a tightly integrated M&O organization to support end-users and systems, such as application operations, which includes (but is not limited to) the following:

- Performance monitoring and tuning
- Monitoring and error handling
- Release management and deployment
- Coordinated scheduling of maintenance and change deployment
- Batch executions
- Service requests and ad-hoc data requests
- Incident management
- Database change request (DBCR) execution
- Integration support for 47 business partners
- Outage resolution
- Upgrades for the base product
- Patching and upgrades
- Asset and configuration management
- Capacity management

- Application lifecycle management including maintenance of the program's Application Lifecycle Management (ALM) tool
- Maintenance of documentation and runbooks
- Auditing

Accenture provides a tightly integrated infrastructure organization to support Ohio Benefits, and is responsible for the following functions as the prime infrastructure contractor:

- **Infrastructure Operations:** Environment management, capacity management, performance tuning, monitoring and error handling, patching and upgrades, and asset and configuration management
- **Application Operations:** Batch operations, documentation and runbooks, integration with state, agency or external interface partners/systems, and incident/problem and defect management
- **Service Desk:** A multi-tiered service desk
- **Security:** Auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management

Interoperability

As interoperability at the service desk impacts every part of Ohio Benefits, our work to support the infrastructure has been similarly broad. Ohio Benefits implements over 85 interfaces across 47 partners, including both state and federal partners, such as the IRS and SSA. Batch and real-time interfaces are implemented leveraging Axway API gateway. Interoperability enables Ohio Benefits to exchange data and information with external systems, products, and data sources. The service desk Tier 3 resolver teams ensure incidents across platforms are mapped to the correct team.

Project #2	Contact #2
Company Name: U.S. Department of Treasury Internal Revenue Service	Contact Name: [REDACTED]
Project Name: Integrated Enterprise Portal (IEP) 1.5 Program	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) IEP 1.0 May, 19, 2011 through May, 18, 2017 IEP 1.5 February, 15, 2017 through February, 14, 2025	Address: [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 164 months	Phone Number: [REDACTED]

Contract Amount: Exceeds \$1,000,000,000	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture has 10 years and three months of prime contractor experience performing service/help desk activities using the Information Technology Infrastructure Library (ITIL) standards and framework, supporting Tiers 1 and 2 service desks, as well as security, maintenance, and interoperability at Federal Treasury IEP, a system that meets the definition of a large and complex IT system. Therefore, our experience on IEP exceeds the requirement as one of two projects needed for F3.</p> <p>PROJECT DESCRIPTION</p> <p>The IEP 1.5 Program is the digital front door to the Internal Revenue Service's (IRS) backend systems and provides technology services to thousands of internal and external users. It is mission critical in securely serving taxpayers, tax preparers, and employees. By continuously improving and innovating its platforms and applications through the IEP 1.5 Program, the IRS is sustaining its infrastructure and applications, expanding capabilities, and increasing resiliency.</p> <p>Initially transitioning two portals from another contractor, Accenture's involvement with the IEP began in May 2011 on the IEP 1.0 Program. In February 2017, Accenture partnered with the IRS on the IEP 1.5 Program to perform maintenance and operations of its infrastructure and applications.</p> <p>Technical solution</p> <p>A key component of the IEP 1.5 infrastructure is its ability to deliver a scalable, elastic infrastructure using cloud-based services. The IEP infrastructure is designed to support iterative transformation without service disruption. IEP 1.5 encompasses the following systems and domains:</p> <ul style="list-style-type: none">• Public User Portal (PUP – IRS.gov)• Registered User Portal (RUP)• Employee User Portal (EUP)• Portal Account Replacement Tool (PART)• Affordable Care Act Transactional Portal Environment (ACA-TPE)• Certified Professional Employer Organization (CPEO) & 501(c)(4) Online Registration System• Field Assistance Scheduling Tool (FAST)• 90+ managed applications• 3,500+ servers	

The IEP features a multi-tiered processing architecture, including three user portals optimized for multiple user interface platforms (e.g., laptops and mobile devices). As part of the IEP solution, Accenture integrated over 90 applications, including ServiceNow and CPEO Versa, both of which are COTS applications. Accenture has also integrated five external systems, including the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.

The modernized system is accessed by over 1,000 internal users from multiple locations. During the 2021 filing season (February 12 to May 17, 2021), there were 767.1 million total site visits (from internal and external users) to IRS.gov and 2.02 billion page views on the site. The peak day was March 15, 2021, when 37.3 million visited the site and 88.1 million pages were viewed.

Services delivered

As the prime contractor, Accenture uses AWS cloud services for production applications and manages more than 40 public applications. Accenture is responsible for system modifications, hardware/software, project management, and cloud-based operations activities such as network and system engineering, cybersecurity vulnerability mitigation, capacity planning, performance testing and monitoring, and batch processing. Accenture also supports security, maintenance, and interoperability. The large and complex Federal Treasury IEP Program contract value exceeds \$1 billion and is ongoing through February 2025.

Using the Information Technology Infrastructure Library (ITIL) as the service desk framework, Accenture provides Tier 1 and Tier 2 service desk support for the IEP non-production environments. The IEP service desk supports request fulfillment, incident management, problem management, and asset management. Additionally, the IEP service desk provides initial support for all IEP-related incidents, including opening tickets in the ITSM system to coordinate with other IRS organizations for incidents outside of the IEP purview.

Accenture created the IRS.gov website Help Desk, which serves as a “first aid station” for IRS.gov website questions such as navigation of IRS content and forms retrieval. The IRS.gov website Help Desk is a complementary service to the IRS toll-free tax assistance line. Accenture successfully delivered the IRS.gov website Help Desk for the IRS for 15 years and acted as the front door for many IRS.gov website visitors in their interactions with IRS.

Accenture collaborates in a multi-contractor environment with five other contractors responsible for different areas of the IEP. Accenture works with contractors such as Leidos, Deloitte, and Booz Allen to manage and maintain the IRS' infrastructure and coordinate the five legislatively mandated applications currently under development in the IEP's AWS-managed service cloud (two of which are Accenture-managed). Accenture is currently migrating legislatively mandated applications to the cloud and is expected to complete the migration of the remaining applications by January 2023.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The IEP solution integrates with over 90 applications. ServiceNow and CPEO Versa are two of the top COTS applications. In addition, PART is a care act identity management COTS product and FAST is the ServiceNow COTS product.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The IEP solution interfaces with five external systems, hosted by Health and Human Services for Medicare & Medicaid Services (HHS CMS) and IRS back-end systems. The applications include but are not limited to the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.
3. **Is accessed by at least 1,000 users at multiple locations:** The IEP solution is accessed by more than 1,000 users at multiple locations. The PUP—the IRS external or internet portal, IRS.gov, that allows unrestricted public access to non-sensitive materials and applications had 2.02 billion page views and 767.1 million total visits during the 2021 filing season (February 12–May 17, 2021).
4. **Has a contract value of at least \$10,000,000 dollars:** The IEP solution contract value exceeds \$1 billion.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The IEP solution features multi-tiered processing, including a user facing front-end optimized for multiple user interface platforms. There are three main portals: PUP, registered user portal, and employee user portal. The ACA Application-to-Application (A2A) is a core interface.

I-F3 EXPERIENCE DETAILS

Accenture has performed service desk activities for Federal Treasury IEP since September 2012. These activities include using the ITIL standards and framework, supporting Tier 1 and 2 service desks, security, maintenance, and interoperability. We have a service desk for all infrastructure support, and it integrates with the client service desk. Service desk activities are currently ongoing through February 14, 2025.

Using ITIL standards and framework

For the IRS, we employ the ITIL standards and framework, along with the National Institute of Standards and Technology (NIST) Risk Management Framework (which also includes ITIL), for over 10 years. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally. These best practices are embedded in our Accenture Delivery Methods, which is the foundation for our infrastructure consulting methods.

In terms of NIST, we maintain an active ATO for IEP 1.5 and will continue to work with the IRS Authorizing Official Certification Program Cyber Office (CPO), and Security Assessment Services (SAS) to support future enhancements. Additionally, we have successfully gone through the FedRAMP Agency Authorization process to obtain ATOs for multiple IRS cloud applications.

Accenture continues to follow the NIST Risk Management Framework guidelines documented in NIST 800-37 as we operate the IEP 1.5 to meet Security Risk Management Framework requirements. Through various continuous monitoring techniques, we continue to ensure the systems we manage are compliant with the security policies outlined in IRM 10.8.1, IRM 10.8.24, and NIST 800-53 Rev.5.

ISO 20000 (previously published as BS15000) is an international standard for IT Service Management based on ITIL. While ISO 20000 defines the requirements for service providers to plan for and deliver managed services, it also represents an industry consensus to help prepare for audits against ISO 20000. Accenture has achieved the ISO 20000 certification in multiple locations. The use of ITIL on the IEP project promotes the adoption of an integrated process approach to effectively deliver infrastructure services to meet business and customer requirements.

Service desk experience, including supporting Tiers 1 and 2 service desks/help desks

Accenture provides Tier 1 and Tier 2 service desk (SD) support for our non-production environments at IEP. The IEP SD serves as the initial point of contact for IEP services, incidents, and problems and provides 24/7/365 support for IEP environments. The IEP SD business hours for support for IRS non-production environments are Monday through Friday from 9 a.m. until 6 p.m. Eastern US time. The IEP SD uses an ITIL framework to support request fulfillment, incident management, problem management, and asset management. The IEP SD provides initial support for all IEP-related incidents, including opening tickets in the client-hosted ITSM system to coordinate with the other IRS organizations for incidents outside of the IEP purview. The Tier 1 service desk triages the ServiceNow case, categorizes the issue, and attempts to resolve the case. If the Tier 1 Service Desk cannot resolve the ServiceNow case, a ServiceNow incident is created and escalated to the Tier 2 Service Desk for resolution. We have a Tier 2 service desk for all production-level incidents and utilize the IRS' incident management system.

We work with all the IRS parties through the Service Restoration Team (SRT) process to bring issues to resolution, with minimal business impact on the customer and within agreed service levels and business priorities. While the SD is focused on incident management and restoration of service, they still integrate with our other processes (e.g., change management and end-to-end monitoring) to provide end-to-end support of issue resolution. IEP ensures visibility into SD operations processes by enabling access to the Service Desk Standard Operational Procedure (SOP). The SOP is reviewed and updated on a periodic basis to maintain its accuracy as the IEP and its processes evolve.

Accenture created the IRS.gov website Tier 1 Help Desk, which serves as a "first aid station" for IRS.gov website questions such as navigation of IRS content and forms retrieval during operating hours of 8 a.m. to 8 p.m. Eastern time Monday through Friday. Taxpayer inquiries are handled via call, email, and chat channels. The IRS.gov website Help Desk is a complementary service to the IRS toll-free tax assistance line and, therefore, does not respond to tax questions or personal inquiries. Accenture successfully delivered the IRS.gov website Help Desk for the IRS for 15 years and acted as the front door for many IRS.gov website visitors in their interactions with IRS.

Accenture's custom solutions for IEP ensure that all end-users are provided the level of support to accelerate resolution as quickly as possible.

Security

The service desk is alerted when security incidents are detected. The Security Operation Center (SOC) will receive a ticket/notification to investigate the incident of a potential breach. Once they have completed their investigation and remedy the security-related issue, they notify the service desk, and the ticket is closed. Examples of security related incidents include unusual behavior of privileged user accounts; unauthorized insiders trying to access servers and data; phishing anomalies in network traffic; excessive consumption of server memory; unauthorized changes in configuration and unexpected account lockouts and password changes. The service desk works in collaboration with the SOC to ensure all aspects of security are communicated and resolved across the ecosystem.

In addition, Accenture supports vulnerability scanning, penetration testing, and IV&V of security controls for applications hosted on the IEP 1.5 platform. There are three primary phases to IEP's approach to manage vulnerabilities: identification, prioritization, and patch deployment. For identification, we use multiple security tools and notifications from IRS Security or other third parties. For prioritization, Accenture uses a risk matrix (outlined in the Internal Revenue Manual) that provides a customized risk score based on various inputs. Patch deployment is based on the results of prioritization. Accenture completes the development, testing, and deployment of patches in the timeframes defined.

Accenture updates antivirus definitions in an automated way; updates are applied as they come available from the vendor. Accenture also monitors both industry and government sources for information on new and emerging threats. As emerging threats are identified, we evaluate their applicability to the IEP 1.5 solution. When applicable, we update the overall Portal threat model and use our various security tools to determine if the threat is present in the environment. If the threat is confirmed, we evaluate options for prevention and work with the IRS to determine the next steps for the implementation.

Accenture has a documented Access Management Plan in place to ensure the right users have the right access in the right roles. The plan uses multiple tools to provide a scalable, secure bastion host platform for day-to-day administration needs in the environment, including handling regular provisioning and deprovisioning activities. This process includes a multi-step approval process to validate clearance levels, business need, and separation of duties across the platform. We review, update, and submit the Access Management Plan as defined in the deliverable schedule at least annually. The solution also includes certificate management procedures in place to manage internal IEP certificates and to deploy application-managed certificates through the IEP application deployment process. Accenture enhanced the IEP's security posture by implementing advanced bot detection, dynamic application scanning, IRS security incident response center visibility and communications, and HSPD12 enablement.

Maintenance

Accenture manages any changes in the IT infrastructure via the IRS Change Management tool and our change management review and approval processes. With IEP 1.5, we increased the managed services delivery aspect through minimized touchpoints for greater efficiency and accountability via SLOs. IEP 1.5's change management process for the IT infrastructure provides IRS visibility and interaction at a level far greater than the typical change management process used in a standard commercial/public managed service approach. This is achieved through tightly integrating the Accenture and IRS change management processes, with supporting reports and transparency.

We regularly execute technical changes, ranging from patching to performance tuning, to other changes. We execute these changes in alignment with the IEP and government/agency standard change management process and review them to confirm compliance with requirements, create change requests, and coordinate required changes through the IRS Change Management process as needed. As of April 2021, results from the Acceptable Quality Levels (AQL) since the inception of the program include:

- 95% of production application deployments shall be performed within the agreed upon schedule and the application does not have issues caused by web hosting platform services: This has been exceeded with an average score of 100%.
- 95% of Non-Production Service Requests completed within set time requirements (varies based on request type): This has been exceeded with an average score of 99.5%.

Interoperability

The service desk helps ensure interoperability incidents across platforms are mapped to the correct team. The IEP solution integrates with over 90 applications. ServiceNow and CPEO Versa are two of our top COTS applications. In addition, PART is a care act identity management COTS product and FAST is the ServiceNow COTS product. The IEP solution interfaces with more than five external systems including the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.

Project #3	Contact #3
Company Name: State of Kansas, Department of Health and Environment (DHE)	Contact Name: [REDACTED]
Project Name: Kansas Eligibility Enforcement System (KEES)	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) September, 1, 2011 through August, 31, 2024	Address: [REDACTED] [REDACTED]

Contract Duration (months): 155 months	Phone Number: [REDACTED]
Contract Amount: Greater than \$100,000,000	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>As of January 4, 2023, Accenture has nine years and two months of prime contractor experience performing service/help desk activities for Tiers 1, 2, and 3 using Information Technology Infrastructure Library (ITIL) standards and framework for the Kansas Eligibility Enforcement System (KEES), a system that meets the definition of a large and complex IT system. Our experience on KEES exceeds the requirement as one of the two projects needed for F3.</p> <p>PROJECT DESCRIPTION</p> <p>KEES is a health and human service eligibility system that was developed and implemented to administer the full suite of human service programs. The system first went live in a phased approach, with its first go-live in July 2012 and the final go-live in 2017. This includes Food Assistance (SNAP), Temporary Assistance for Needy Families (TANF), Child Care, Employment Services, Food Assistance, Employment and Training (FAET and GOALS), Low Income Energy Assistance Program (LIEAP), Automated IV-E Eligibility, Medical assistance programs, including Medicaid (MAGI, E&D, and LTC), CHIP, KanCare, AIDS Drug Assistance Program (ADAP), and several other state-funded programs.</p> <p>The Kansas Department of Health and Environment's (DHE) Division of Health Care Finance and the Kansas Department for Children and Families (DCF) administers human service and medical assistance (MA) programs that serve over 720,000 Kansans annually. In the last two years, the KEES has distributed over \$814 million in benefits to Kansans.</p> <p>The KEES system provides Kansans with greater integration across its programs and online access to health information as an alternative to office visits. The system generates savings through more efficient eligibility processing and much-improved decision-making and compliance controls. Through a flexible and modular technology approach, KEES helps the state more readily and cost-effectively update the eligibility system as Kansan's needs and government policies change over time.</p> <p>Technical solution</p> <p>In January 2020, Accenture transferred KEES onto Oracle Cloud after a nine-month design and implementation process. Within Oracle Cloud, Platform as a Service (PaaS) and Software as a Service (SaaS) are used for application delivery. The Core Logging as a Service (LaaS) solutions aggregate components run on Linux and Microsoft Windows. The large and complex solution integrates custom code with multiple COTS applications (e.g., Adobe Experience Manager, Oracle Intelligent Advisor, Oracle Address Verification, Oracle Analytics, Stone Branch, etc.), including the citizen-facing portal, worker eligibility system, and COTS eligibility software.</p>	

This platform has several portals supported by multi-tiered processing, including a user-facing application optimized for multiple user interface platforms (e.g., laptops and mobile devices). The platform interfaces with over 25 major external systems, including state and local partners for income information, federal partners for social security data, the KMMS (MMIS) system for Kansas, and the federal hub (which is real-time). There are 2,500 internal and tens of thousands of external users in multiple locations.

Services delivered

Accenture's contract began in September 2011 and is ongoing through August 31, 2024. As the prime contractor for KEES, Accenture performs application maintenance, system modifications, cloud-based operations, cybersecurity vulnerability mitigation, network and system engineering, capacity planning, performance testing, performance monitoring, and batch processing. Accenture is also responsible for application design, development, testing, change management, training, conversion, and running a service desk (tiers 1, 2, and 3 via ServiceNow) using the Information Technology Infrastructure Library (ITIL) standards and framework. Accenture continues to serve as the prime maintenance and operations vendor responsible for ongoing system maintenance, security, deployments, and enhancements providing day-to-day system operations through effective project management, governance, and communication with Kansas DHE.

Accenture has implemented innovative solutions outside of their original scope, such as digital imaging and artificial intelligence (AI) bots. Accenture is overseeing a project at Kansas DCF to develop an Amazon Chime chat and an enhanced virtual contact center to provide Kansans with an enhanced customer service experience, and to enable agents to handle increased call volume from anywhere.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The KEES platform integrates custom code with multiple COTS applications, including Adobe Experience Manager, Oracle Intelligent Advisor, Oracle Address Verification, Oracle Analytics, Stone Branch. It also integrates with the citizen-facing portal, worker eligibility system, and COTS eligibility software.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The platform interfaces with over 25 external systems, including state and local partners for income information, federal partners for social security data, the KMMS (MMIS) system for Kansas, and the federal hub (which is real-time).
3. **Is accessed by at least 1,000 users at multiple locations:** The KEES solution is accessed by 2,500 internal users and tens of thousands of external users in multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The KEES contract value is greater than \$100,000,000.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** KEES includes a multi-tiered architecture with multiple front-end applications supporting a variety of user interface platforms (e.g., laptops and mobile devices).

I-F3 EXPERIENCE DETAILS

Accenture has been performing service desk activities for KEES since Fall of 2013. These activities include using Information Technology Infrastructure Library (ITIL) standards and framework, supporting Tiers 1, 2, and 3 support, security, maintenance, and interoperability. Service desk activities are ongoing through August 2024.

Using ITIL standards and framework

For the KEES system, we employ the Information Technology Infrastructure Library (ITIL) standards and framework. This provides a cohesive set of best practices, drawn from the public and private sectors internationally as the most widely accepted approach to IT service management in the world. Accenture Delivery Methods has incorporated ITIL best practices and terminology, with ITIL as the foundation for our Infrastructure Consulting methods. Accenture has thousands of individuals trained in ITIL and has been actively involved with the IT Service Management Forum, the ITIL user group, as well as the Office of Government Commerce (OGC) as the owner of ITIL. Alongside Carnegie Mellon University, Accenture is a co-author of the Service Strategies book, one of the five volumes in ITIL v3.

ISO 20000 (previously published as BS15000) is an international standard for IT Service Management based on ITIL. While ISO 20000 defines the requirements for service providers to plan for and deliver managed services, it also represents an industry consensus to help prepare for audits against ISO 20000. Accenture has achieved the ISO 20000 certification in multiple locations. The use of ITIL on the KEES account promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements.

Service desk experience, including supporting Tiers 1 and 2 service desks/help desks

At KEES, we provide a fully operational service desk. It is based on a multi-tier service desk model and is organized into three tiers: Tier 1, 2 and 3. Each tier of the model works as follows:

- Tier 1 is the initial contact point for interactions with the Service Desk. Tier 1 will create cases for each interaction, triage, categorize the case, attempt to resolve and, if necessary, escalate to Tier 2 with the creation of a related Incident. This tier is supported through two methods described subsequently in further detail.
- Tier 2 will review the escalated Incident and attempt to resolve. Upon resolution, the incident and related case(s) are all closed. For incidents that cannot be resolved by Tier 2, Tier 2 will escalate to Tier 3 for resolution.
- Tier 3 is staffed with our application development, production operations and technical subject matter experts. Tier 3 will create an incident ticket, assign to the appropriate expert for application fixes or workarounds. Upon resolution, the problem and related incident(s) and case(s) are all closed.

This service desk model sees that end-users are provided the level of support to accelerate resolution.

Although not part of KEES, Accenture established an Amazon Connect solution for Kansas in response to COVID-19, migrating help desk services to home offices. This helped a state non-medical agency call center securely take calls from home. Recently,

Amazon Chime has been added that allows video calls and remote video takeover to view and resolve the customer's issues. This solution enables chat and can provide content about the caller to the call center worker. This helps efficiently and accurately answer the customer's questions based on the content of the chat.

Security

An information security program providing confidentiality, integrity, and availability is critical to the KEES Program. The State of Kansas provides the policies that we must adhere to when designing, developing, implementing, and operating KEES. These policies are based on National Institute of Standards and Technology (NIST) cybersecurity and FedRAMP System Security standards. Other requirements come from flow-down laws and regulations from third-party agreements. The State of Kansas Chief Information Security Officer has oversight responsibilities that include the testing and validation of the vendor implementation of the NIST SP 800-53 security controls. In addition, the client security team performs periodic audits focused on technical vulnerabilities.

Security services provided by Accenture include:

- Security incident response, including a 24/7/365 response capability to address security incidents based on severity and impact to the confidentiality, integrity, and availability of the system
- Continuous security vulnerability scanning and remediation within required timeframes, including coordination with infrastructure and application release management activities
- Access Control, including regular access control audits of users provisioned to roles and permissions assigned to roles
- Specialized security role training for vendor and subcontractor personnel employed in security role
- Monitoring and alerting provided by a centralized Security Information and Event Monitoring system that is monitored 24/7
- Security assessment of all modifications, changes, and acquisitions for the System
- Regular auditing of system configurations and changes, to confirm an accurate accounting of all System components and proper execution of change management processes
- Security integration with contingency planning and disaster recovery activities and testing
- Operation and maintenance of identity management systems that provide authentication and authorization functions across KEES' supporting infrastructure

The State of Kansas leads the architectural standards Review Sessions to confirm accountability, transparency, responsiveness, inclusiveness, empowerment, and broad-based participation in the development of Secure Architectural Standards. They facilitate the approval process and adoption of standards.

This team also supports the independent third-party technical security audit performed on a regular basis. The audits assess that:

- Implementation of controls is documented with evidence to prove compliance to the control

- All technical systems properly implement the security control according to the Center for Internet Security (CIS) controls benchmark standard for the appropriate technology
- The non-technical controls are properly implemented according to the processes documented in compliance with NIST CyberSecurity Framework, ISO27002, SOC2 and applicable security policies, standards, and control baselines
- Any known deficiencies are properly documented with Plan of Actions and Milestones (POAMs) created to track their remediation
- A report will detail the results categorized by each NIST control family and provide the remediation for the security control according to the CIS benchmark

Maintenance

Accenture manages any changes in the infrastructure via the KEES change management review and approval processes. We regularly execute technical changes, ranging from patching to performance tuning, and other changes. We execute these changes in alignment with the Kansas change management process and review them to confirm compliance with requirements, create change requests, and coordinate required changes. KEES is available and accessible 24/7/365 except for scheduled downtime. The maintenance of the knowledge base has been architected to refresh periodically with the latest content library includes tutorials that guide the user step by step through how to use key software features and resolve simple errors they might encounter. Requests to approve scheduled downtime will go through the KEES Operations Team and confirmed with the business. Prior to scheduled downtime, diligent planning activities are completed to provide a greater lead time and minimize the actual scheduled downtime. Service desk maintenance is comprised of identifying the improvements needed when it comes to people, process, and procedures. Maintenance is a continuous improvement process to ensure that the residents and workers have the latest information, policies, and features. Accenture has demonstrated expertise with implementation, maintenance, and operation of the following technologies for KEES:

- Oracle Cloud environment
- Linux and Windows VMs in the Oracle Cloud Environment
- Oracle database
- Oracle Exadata
- Oracle WebLogic Oracle Service Bus

Interoperability

The service desk helps ensure that interoperability incidents across platforms are mapped to the correct team. KEES integrates several applications, including the APSP suite for eligibility, which is a COTS. This suite has several portals and many dependencies, interfaces, and exchanges with external systems. These external systems include many federal Centers for Medicare and Medicaid Services, state data integrations, and external private services such as FIS (for EBT card integration) and TALX (for income verification). KEES also includes a multi-tiered architecture with multiple front-end applications supporting a variety of user

interfaces, some of which are real-time. Accessed daily by thousands of users in multiple locations, KEES has a large set of functional capabilities and elaborate data relationships.

Project #4	Contact #4
Company Name: California Statewide Automated Welfare System (CalSAWS) Consortium	Contact Name: [REDACTED]
Project Name: California Statewide Automated Welfare System (CalSAWS) (prior project name was the LEADER Replacement System (LRS), which is now called CalSAWS)	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) LRS/CalSAWS November, 7, 2012 through April, 30, 2025	Address: [REDACTED] [REDACTED]
Contract Duration (months): 149 months	Phone Number: [REDACTED]
Contract Amount: LRS/CalSAWS \$1,425,495,842	Email: [REDACTED]

Describe the services provided:

EXPERIENCE SUMMARY

As of January 4, 2023, Accenture has 10 years of experience performing service/help desk activities using Information Technology Infrastructure Library (ITIL) standards and framework at CalSAWS, a system that meets the definition of a large and complex IT system. Therefore, our experience on CalSAWS alone **exceeds the requirement** stated in F3.

PROJECT DESCRIPTION

CalSAWS is an integrated eligibility system built and operated by the CalSAWS Consortium on behalf of the 58 counties of California. CalSAWS supports the counties in administering public assistance programs in California, including cash assistance (CalWORKs/TANF), food assistance (CalFresh/SNAP), medical assistance (Medi-Cal/Medicaid), and other state and county-specific programs. The system first went live in 2015 in Los Angeles County, and at that time, it was known as the LEADER Replacement System (LRS). Migration from an on-premises data center to cloud hosting occurred on October 14, 2019.

Technical solution

CalSAWS is the most extensive integrated eligibility system in the United States and is hosted in the Amazon Web Services (AWS) cloud. Supporting over 10 million transactions daily, CalSAWS has more than 50 interfaces, six of which are real-time. The system is currently in production in 42 counties. The system is used by 18,500 internal users daily across 125 locations to support 11 million Californians who receive public assistance. CalSAWS issues more than \$1 billion in benefits each month. By October 2023, all 58 counties will have migrated to this platform. After all counties are migrated to CalSAWS, 41,000 internal users will use CalSAWS daily to support approximately 19 million Californians and issue approximately \$2 billion in benefits each month.

Services delivered

Accenture is one of six contractors responsible for CalSAWS and has the largest scope of work. Accenture's contract began in November 2012 and is ongoing through April 2025. As the prime contractor for systems integration and maintenance and operations (M&O), Accenture is responsible for application maintenance and system enhancements, and cloud-based operations including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing and monitoring, and batch processing. Accenture supports hardware and software management, system engineering, data conversion, and project management. Accenture also supports the service desk (tiers 1, 2 and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework.

Accenture is responsible for the core CalSAWS eligibility system, the analytics application, ForgeRock identity solution, contact center technologies, the Child Care Provider Portal, and kiosks/tablets in several county lobbies. The CalSAWS Consortium has separate prime contracts for the legacy system maintenance (CalWIN), cloud hosting, the public portal (BenefitsCal), imaging (SaaS contract), OCAT, GA/GR Correspondence solution, and print services.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CalSAWS solution integrates custom Java code with COTS applications (e.g., Oracle database and middleware products, Informatica Identity Resolution, Pitney Bowes Spectrum, ForgeRock, and IBM Operational Decision Manager). The core eligibility application further integrates with other COTS applications (e.g., Adobe Experience Manager and AWS Connect) and custom applications (e.g., OCAT, Child Care Portal, and BenefitsCal).
2. **Interfaces with at least five external systems, at least one of which is real-time:** The CalSAWS solution interfaces and exchanges with 50 external systems. BenefitsCal, CalHEERS, County Master Data Management (MDM), Lobby Monitors, the Online CalWORKS Appraisal Tool (OCAT), and Statewide Client Index all interface in real time.
3. **Is accessed by at least 1,000 users at multiple locations:** The CalSAWS solution is accessed by an average of 18,500 daily users across 125 locations. After the CalWIN counties are migrated, the number of CalSAWS users will be approximately 41,500.
4. **Has a contract value of at least \$10,000,000 dollars:** The CalSAWS contract value is \$1,425,495,842.

5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:

The CalSAWS core eligibility application includes a multi-tiered processing architecture, a presentation tier optimized for multiple user interface platforms (e.g., Google Chrome and Microsoft Edge), an application tier, and a data tier. Other components of the system run on other user interface platforms such as kiosks and tablets.

I-F3 EXPERIENCE DETAILS

Accenture has been performing service desk activities for CalSAWS since the beginning of the project in November 2012 when it was called LRS. These activities include using the ITIL standards and framework, and supporting Tiers 1, 2, and 3, as well as security, maintenance, and interoperability. Service desk activities are currently ongoing.

Using ITIL standards and framework

The Accenture Delivery Methods, which help define how we deliver services to all our clients—including at CalSAWS, incorporate ITIL best practices and terminology. We also use ITIL best practices as the basis for our Infrastructure Consulting methods used when providing IT service management consulting services to our clients. We recognize that ISO 20000 (previously published as BS15000) is an international standard for IT Service Management based on ITIL. The use of ITIL on the CalSAWS account promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements. While ISO 20000 defines the requirements for a service provider to deliver managed services, it also represents an industry consensus on guidance to auditors and helps service providers planning service improvements or to be audited against ISO 20000. Accenture has achieved ISO 20000 certification in multiple locations.

Service desk experience, including supporting Tiers 1 and 2 service desks/help desks

At CalSAWS, we have a fully operational service desk that supports Tier 1, 2, and 3. We are the prime and we work with our subcontractor, Gainwell, to provide service desk functions. The CalSAWS Service Desk model has two Tier 1 methods. Some CalSAWS counties operate their own local Tier 1 County Help Desk. The Tier 1 County Help Desk will triage the ServiceNow case, categorize the issue, and attempt to resolve. If the Tier 1 County Help Desk cannot resolve the ServiceNow Case, a ServiceNow Incident is created and escalated to the CalSAWS Tier 2 Service Desk for resolution. For those counties that do not operate a local Tier 1 County Help Desk, the CalSAWS Service Desk provides the Tier 1 service and will create ServiceNow cases for the reported issues, categorize the issues, and attempt to resolve them. The CalSAWS Central Service Desk uses a multi-tier model, organized into three tiers.

- Tier 1: For counties with no county help desk, Tier 1 is the initial contact point for interactions with the CalSAWS Service Desk. Tier 1 will create ServiceNow cases for each interaction, categorize the case, attempt to resolve and, if necessary, escalate to Tier 2 with the creation of a related ServiceNow incident. This tier is supported through the two methods previously described.
- Tier 2: Tier 2 will review the escalated incident and attempt to resolve the incident. Upon resolution, the incident and related case(s) are all closed. For incidents that cannot be resolved by Tier 2, Tier 2 will escalate to Tier 3 for resolution.

- Tier 3: Tier 3 is staffed with contractor application development, production operations, and technical subject matter experts. Tier 3 will create a ServiceNow problem and assign the problem to the appropriate expert for an application, hardware, software, or connectivity/network fix. Upon resolution, the problem and related incident(s) and case(s) are all closed.

As a result, the custom solution for CalSAWS ensures that all end users are provided the level of support needed to accelerate resolution.

Today, there are 14 California counties with call centers and a total of 1,200 agents in those counties. We are onboarding the additional 18 CalWIN counties plus LA county (a total of 19) and onboarding an additional 8,502 agents to those 19 counties. We anticipate a total of 9,702 agents after onboarding.

Security

The service desk is alerted when security incidents are detected. The Security Operation Center (SOC) will receive a ticket/notification to investigate the incident of a potential breach. Once they have completed their investigation and remedy the security-related issue, they notify the service desk, and the ticket is closed. Examples of security related incidents include unusual behavior of privileged user accounts; unauthorized insiders trying to access servers and data; phishing anomalies in network traffic; excessive consumption of server memory; unauthorized changes in configuration and unexpected account lockouts and password changes. The service desk works in collaboration with the SOC to ensure all aspects of security are communicated and resolved across the ecosystem.

An information security program providing confidentiality, integrity, and availability is critical to the CalSAWS program. The Consortium provides the policies that contractors must adhere to when designing, developing, implementing, and operating CalSAWS. These policies are based on National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 4, the customized CalSAWS System Security Plan (SSP) which meets the specifications for the FedRAMP System Security Plan for Moderate Classification Systems, and flow-down laws and regulations from the CalSAWS Privacy and Security Agreements with CDSS and DHCS. The CalSAWS Chief Information Security Officer has oversight responsibilities that include the testing and validation of the vendor implementation of the NIST SP 800-53 security controls. In addition, the Consortium Security team performs audits periodically focused on technical vulnerabilities for the overall CalSAWS program and interconnected system. This team also supports the independent third-party technical security audit performed on a regular basis. The audits assess that:

- the implementation of each control is documented with evidence to prove compliance to the control.
- all technical systems properly implement the security control according to the Center for Internet Security (CIS) controls benchmark standard for the appropriate technology.
- the non-technical controls are properly implemented according to the processes documented in compliance with NIST CyberSecurity Framework, ISO27002, SOC2 and CalSAWS security policies, standards, and control baselines.

- any known deficiencies are properly documented with plans of action and milestones (POAMs) created to track their remediation.

A report details the results categorized by each NIST control family and provides the remediation for the security control according to the CIS benchmark. The Consortium leads the CalSAWS Architectural Standards Review Sessions to confirm accountability, transparency, responsiveness, inclusiveness, empowerment, and broad-based participation in the development of CalSAWS Secure Architectural Standards. The Consortium facilitates the approval process and adoption of standards.

Security services provided by Accenture for CalSAWS currently include the following:

- Access control, including regular access control audits of users provisioned to roles and permissions assigned to roles
- Specialized security role training for vendor and subcontractor personnel employed in security roles
- Monitoring and alerting provided by a centralized Security Information and Event Monitoring (SIEM) system that is monitored 24/7, with ingestion from across CalSAWS and resources
- Security assessment of all modifications, changes, and acquisitions for the system
- Regular auditing of system configurations and changes to confirm an accurate accounting of all system components and proper execution of change management processes
- Security integration with contingency planning, disaster recovery activities, and testing
- Operation and maintenance of centralized identity management systems that provide authentication and authorization functions across CalSAWS and the supporting infrastructure
- Security incident response, including a 24/7/365 response capability to address security incidents based on severity and impact to the confidentiality, integrity, and availability of the system
- Continuous security vulnerability scanning and remediation within required timeframes, including coordination with infrastructure and application release management activities
- Physical security for all CalSAWS data sites, including security monitoring, physical access control, and physical security auditing

Maintenance

The CalSAWS system is available and accessible 24/7/365, except for scheduled downtime. The CalSAWS system is architected to be up when CalSAWS nightly batch is running. The maintenance of the knowledge base has been architected to refresh periodically with the latest content library includes tutorials that guide the user step by step through how to use key software features and resolve simple errors they might encounter. Requests to approve scheduled downtime go through the CalSAWS Project's Tech Change Advisory Board (CAB) process. The goal is to do planning upfront to provide as much lead time as possible to notify the counties of scheduled downtime. Service desk maintenance is comprised of identifying the improvements needed

when it comes to people, process, and procedures. Maintenance is a continuous improvement process to ensure that the residents and workers have the latest information, policies, and features.

Accenture provides a tightly integrated M&O organization to support CalSAWS and is responsible for the following functions as the prime M&O contractor:

- **Infrastructure operations:** Environment management, capacity management, performance tuning, monitoring and error handling, patching and upgrades, asset and configuration management
- **Application operations:** Batch operations, documentation and runbooks, integration with state, agency, or external interface partners/systems, and incident/problem and defect management
- **Service desk:** Implementing and operating a multi-tiered service desk
- **Security:** Auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management

Prior to combining the various systems, Accenture served as the prime M&O vendor for LRS. The scope of M&O services included data center hosting and operations prior to migration to the cloud, batch operations and monitoring, print center and mail fulfillment operations, performance monitoring, measurement and maintenance, common infrastructure and desktop, managed desktop and server configuration with remote control capability, release management of a bi-monthly release schedule, coordinated scheduling of maintenance and change deployment, integrated enterprise monitoring and management framework, Tier 3 LRS Application Helpdesk, hardware and software procurement, and maintenance.

As a result, for over two decades, Accenture has demonstrated expertise with implementation, maintenance, and operation of the following technologies for CalSAWS and its predecessor systems:

- Oracle Database and Middleware Products
 - Oracle Database Enterprise Edition - 19c
 - Oracle WebLogic Server - 12.2.1.4.0
 - Oracle JDK and JVM - Java 1.8.0.333
 - Oracle OEM (Oracle Enterprise Manager)
- Adobe Experience Manager (SaaS)
- Windows Servers: Windows Server 2016/2019
- BMC Control-M (used until January 2019, at which point CalSAWS migrated to BICsuite Professional)
- Informatica: CalSAWS uses Informatica 10.2 to provide person data search capabilities

Interoperability

The service desk has Tier 3 teams to ensure that interoperability incidents across platforms are mapped to the correct team. The CalSAWS solution interfaces and exchanges with 50 external systems. BenefitsCal, CalHEERS, County Master Data Management (MDM), Lobby Monitor, the Online CalWORKS Appraisal Tool (OCAT), and Statewide Client Index all interface in real time. As interoperability affects every part of CalSAWS, our work to support the infrastructure for interoperability has been similarly broad. Interoperability activities enable CalSAWS to work with other systems or products to exchange data or information. On our infrastructure team, interoperability is important because it enables CalSAWS to exchange data and information with external systems, products, and data sources. Increasing the use of standards-based APIs has created the need for the infrastructure team to manage interoperability challenges and coordination with external applications. Collaboration and communication with the third parties with which we interoperate is critical. With better communication and collaboration, we help maintain interoperability over time.

Project #5	Contact #5
Company Name: State of California–California Department of Public Health (CDPH)	Contact Name: [REDACTED]
Project Name: California Vaccine Management Project (CalVax)	Contact Title: [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) December, 14, 2020 through June, 30, 2023	Address: [REDACTED] [REDACTED]
Contract Duration (months): 30 months	Phone Number: [REDACTED]
Contract Amount: \$280,000,000	Email: [REDACTED]
Describe the services provided:	
EXPERIENCE SUMMARY As of January 4, 2023, Accenture has two years and 11 months of experience performing service/help desk activities using Information Technology Infrastructure Library (ITIL) standards and frameworks at CalVax, a system that meets the definition of a	

large and complex IT system. Service desk activities are currently ongoing through June 30, 2023. Therefore, our experience on CalVax **exceeds the requirement** as one of the two required projects for F3.

PROJECT DESCRIPTION

The California Department of Public Health (CDPH) is a department of the Health and Human Services Agency of the Government of the State of California (the State). CDPH is responsible for public health across the State—setting policy and delivering services to California's 39 million citizens directly or through the State's 61 County or City Local Health Authorities. CDPH delivers services and oversees eligibility determination for a broad range of programs, including public health social services programs like the nutrition program for Women, Infants, and Children (WIC) and the Maternal, Child, and Adolescent Health program. In addition to its social services mandate, the CDPH is the agency charged with overseeing infectious disease control and prevention, leading the State's response to the COVID-19 pandemic.

When COVID-19 vaccines finally became available, California public health officials not only wanted to get them to the public as soon as possible, they set an ambitious goal of aiming to immunize 70% of their 39 million residents within only six months. Accenture launched CalVax in December 2020, a large-scale system integration program to help the State reach this goal.

Technical solution

CalVAX operations is comprised of myCAVax, My Turn, and My Turn Volunteer. The CalVAX solution includes a multi-tiered architecture, including four front-end applications optimized for various user interface platforms. Accenture used MuleSoft as the strategic integration and application programming interface (API) platform. This integration connects with more than seven external systems to integrate the new Salesforce-based vaccine management system with other state and federal systems for the CDPH. Salesforce Lightning Flow Builder, a process automation tool that "calls" MuleSoft's API, is an example of real-time integration delivered by Accenture. The solution interacts with the California Immunization Registry (CAIR2), a COTS solution provided by Gainwell, in real-time to return the validity of healthcare providers. This enabled providers to register in the Salesforce system to order or administer vaccines. This real-time integration helps prevent unauthorized providers from accessing the system and streamlines the registration process that otherwise would require manual intervention.

The My Turn website determines eligibility for vaccines and schedules over 625,000 appointments per month. The My Turn Volunteer website helped volunteers connect with the program to expedite the administration of vaccines. In total, over 10 million vaccination appointments have been scheduled. The myCAVax solution alone supports 20,000 internal end users and 2,000,000 external users at multiple locations.

Services delivered

To support the statewide vaccination campaign, the CDPH joined forces with Accenture, the Federal Emergency Management Agency (FEMA), and Blue Shield of California to develop a secure, integrated vaccine management solution. Through this partnership, more than 50,000 vaccines were administered to residents per day throughout the pandemic. As the prime contractor, Accenture developed and oversaw CalVAX operations. Accenture managed multiple development teams working

in parallel and delivered incremental product features to administer vaccinations as quickly as possible. Using the Agile software development life cycle (SDLC) approach, Accenture configured and launched these solutions in a matter of weeks, with additional critical functionality deployed every two weeks.

Throughout its contract period, Accenture has supported Tier 1, 2, and 3 service desk activities using the ITIL standards and framework. As part of maintenance, Accenture provides a tightly integrated organization to support CalVAX and is responsible for infrastructure operations including environment management, capacity management, performance tuning, monitoring, and error handling, patching and upgrades, and asset and configuration management. Accenture also supports application operations such as batch operations, integration with state, agency or external interface partners/systems, and incident/problem and defect management. Security activities include auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management.

Accenture interacts with four other vendors—Blue Cross/Blue Shield, Maximus, Gainwell, and Lyniate—in a multi-contractor environment for cloud-based areas including interfaces, data stores, software, services, migration, and mining.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CalVAX solution integrates with multiple state and federal systems including CAIR2, a COTS solution provided by Gainwell.
2. **Interfaces with at least five external systems, at least one of which is real-time:** For CDPH, we used MuleSoft to integrate the Salesforce-based contact tracing system with more than seven external systems. The included the state's Disease Surveillance system, multiple local health jurisdictions using API calls, CAIR2 for vaccination history, a SQL Server database system for auditing, a Snowflake system for reporting and analytics, an AWS system that handles virtual agent interaction with residents, and more. The integration to the CAIR2 system is a real-time call from the Salesforce system to check the vaccination history of an individual per the request of a contact tracer working in Salesforce.
3. **Is accessed by at least 1,000 users at multiple locations:** The myCAVax solution alone involves 20,000 internal end users and 2 million external users at multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The CalVax contract value is \$280 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The CalVax solution includes a multi-tiered architecture including front-end applications optimized for various user interface platforms.

I-F3 EXPERIENCE DETAILS

We have been performing service desk activities for CalVax since December 2020. These activities include using ITIL standards and frameworks, supporting Tiers 1, 2, and 3, along with security, maintenance, and interoperability.

Using ITIL standards and framework:

We used ITIL for CalVAX to provide a cohesive set of best practices, drawn from the public and private sectors internationally. It is the most widely accepted approach to IT service management in the world. The Accenture Delivery Methods (ADM), which sets the foundation of our delivery, has incorporated ITIL best practices and terminology. We also use ITIL best practices as the basis for our infrastructure consulting methods that we use when providing IT service management consulting services to our clients.

Service desk experience, including supporting Tiers 1 and 2 service desks/help desks

In late 2020, the State had an emergency need to establish a unified system for administering the vaccine rollout. The State partnered with Accenture to rapidly build and deploy the two integrated systems, the vaccine inventory and ordering system (myCAVax) and the vaccine clinic and appointment scheduling system (My Turn). To support these systems, CalVax established the Vaccine Management Help Desk to provide mission-critical technical support to State healthcare providers and clinics.

Tier 1: Tier 1 creates an incident in ServiceNow and assigns it to a Tier 2 or Tier 3 myCAVax or My Turn group.

Tier 2: Tier 2 is staffed with business analysts (BAs) who are myCAVax, My Turn Clinic, and My Turn Public-Portal subject matter experts. The BAs review the escalated incident and create an investigation in Salesforce. During the investigation, the BAs recreate the issue in a lower environment looking at all aspects of the software functionality to determine if the application is working as expected. If the desired behavior is outside the scope of current functionality, an enhancement of the application will be required to provide the desired outcome. After this is determined, Tier 2 creates a user story in Salesforce to accomplish the following:

- Describe the bug or software defect, including documented steps to recreate the issue in a dev/sandbox environment
- Describe the cause of the issue
- Provide the functional and technical specifications necessary to resolve the issue
- Determine when the code fix can be released to production

Tier 2/Tier 3 (L2/L3 support) is a development team that provides application maintenance for both systems. When the application is not working as expected, or when a “warm handoff” with the myCAVax or My Turn Functional team is needed, Tier 2 assigns the user story to the Tier 3 bucket in Salesforce. Tier 3 can then speak with the client (grooming sessions) to better understand the scope of the additional functionality. This specific process is outside the Service Desk. When necessary, for issues related to other integrations within myCAVax or My Turn (like Skedulo and AWS), the respective Tier 3 teams are engaged to address accordingly. Tier 2 manages the user story until the code-fix has been released or handed off to another team outside the Service Desk. When the software code fixes have been released to production, Tier 2 communicates the findings back to Tier 1 for follow-up and closure. In many cases, Tier 2 communicates status and progress directly with the client.

Tier 3: Tier 3 is staffed with Salesforce and other developers with expertise in Salesforce Community Cloud, Apex Programming language, Copado, and other development, build, and release management skills. L2/L3 support developers are staffed with

contractors with the demonstrated skills needed to provide application support and maintenance to myCAVax and My Turn. Tier 3 reviews the user story to understand the bug or defect. They verify the root cause and use it to determine which code changes need to occur to resolve the issue. They then develop solutions in Salesforce and coordinate with the Release Management team to get the code fixes released as software updates. For escalations, Tier 3 coordinates with Salesforce, Skedulo, and AWS as needed.

Operations Expertise: Cross-functional rapid response teams collaborated to quickly frame the help desk operational infrastructure within 10 days. The Operations team includes Level 1 help desk agents as well as training, workforce management, quality assurance, PMO, and innovation roles.

Rapid Agile Resourcing: Accenture uses internal talent across different functional groups, contracting agencies, and a third-party company, allowing for a quick and efficient onboarding process. Our help desk peaked to more than 260 professionals within four months.

Client Data Protection: We adhere to and maintain all security protocols, avoiding exposure of client data, protected health information (PHI), and personal identifiable information (PII).

The Vaccine Management Help Desk provides system-related technical support to State healthcare providers and clinics, including:

- Troubleshooting technical issues
- Creating business and user accounts
- Coordinating profile maintenance
- Providing storage capacity info
- Ordering
- Transferring/redistribution
- Inventory incident reporting
- Providing system usage guidance to clinic/provider managers and vaccine administrators
- Facilitating incident closure with other vaccine management program teams
- Developing standardized reports for provider organizations
- Supporting the myCAVax provider enrollment process

The help desk channels include phones (voice-over IP), emails, live chat, and an FAQ virtual assistant. The tools used include the My Turn/myCAVax Salesforce platform, Power BI/Tableau, AWS, intelligent voice routing (IVR), and Service Now.

Even under the unique pressure of the COVID-19 pandemic, the rollout was successful. The project is ongoing and has expanded to include additional COVID-19 doses, COVID-19 boosters, and doses for Influenza and Monkeypox. Some specific project successes include:

- Handling 48,187 tickets since January 2021
- Completing 71 million appointments to date
- Continuing to exceed internal KPIs while driving client innovation in operations
 - Customer satisfaction score (CSAT) of better than 9 out of 10
 - Quality of more than 95%
 - Average speed to answer (ASA) of less than 30 seconds
 - Compliance 100%
- Exceeding industry standard of 60% retention for Tier 1 help desk
- Providing continuous improvement and layered additional efficiencies through the ServiceNow Knowledge Base, Innovation Hub, and Agent Handbook
- Onboarding 3,700 provider organizations to myCAvax, including:
 - 11,800 provider locations that directly facilitate ordering process
 - 2,000 targeted provider organizations that serve children populations
- Generating increased application response rates through our outreach efforts that led to the administration of more than \$10 million in grant funding to targeted provider populations

Security

The service desk is alerted when security incidents are detected. The Security Operation Center (SOC) will receive a ticket/notification to investigate the incident of a potential breach. Once they have completed their investigation and remedy the security-related issue, they notify the service desk, and the ticket is closed. Examples of security related incidents include unusual behavior of privileged user accounts; unauthorized insiders trying to access servers and data; phishing anomalies in network traffic; excessive consumption of server memory; unauthorized changes in configuration and unexpected account lockouts and password changes. The service desk works in collaboration with the SOC to ensure all aspects of security are communicated and resolved across the ecosystem.

A comprehensive security program providing confidentiality, integrity, and availability is critical to the CalVax program. All contract and security requirements are outlined in the responsibility traceability matrix. We also constructed a RACI matrix to eliminate gaps in security coverage. Accenture's security program complies with CDPH policies and standards, federal laws, local laws and regulations, and Accenture's policies. We have a Client Data Protection (CDP) program with controls to protect security and privacy that includes controls that must be validated regularly by our key staff.

Risk assessments and compliance with NIST

The security program complies with NIST 800-53 R5 and uses NIST CSF components. A detailed overview of security is maintained in the System Security Plan (SSP). Besides the SSP, our team maintains the Technology Recovery Plan (TRP) to outline key system recovery plans, testing strategies, communication information for key staff, and a coordination plan. We use risk assessments, code scanning, configuration reviews, compliance checklists, leading practices, and Accenture assets to meet security requirements. Risk assessments are completed before the acquisition of outsourcing of information services and whenever significant changes to the system or environment occur that may impact security. All new applications, software, or third-party integrations undergo a similar review process and must be approved by CDPH's enterprise architect and Change Review Board. Our assessments follow guidance from NIST 800-39 Managing Risk from Information Systems and NIST 800-30 Risk Management Guide for Information Technology Systems.

Every six months, we conduct a Salesforce Security Rapid Assessment (SSRA) of Salesforce permission sets, code, metadata, and configuration settings. These risk assessments help CDPH determine the minimum set of controls required to eliminate, reduce, or maintain risks at an acceptable level. We document assessment results, share them with the impacted stakeholders and other CDPH personnel as needed, and track them through remediation. We also conduct an annual NIST 800-53-based risk assessment of the overall program, environment, and connected systems.

The Security team provides support for additional audits or assessment requests from CDPH, helping answer questions about how the system is secured, conducting ad hoc security testing and reviews as requested by CDPH, conducting quarterly reviews of all contract requirements, and provides them for CDPH's review. We work with the CalVax Security team to agree on a schedule for completing assessment findings and corrective actions and document project security risks and issues with the CalVax Security team regularly.

Access control

The security program follows leading practices and Accenture's methodology for delivering a comprehensive security program. This includes a strong focus on access control (like access reviews, onboarding, offboarding, role-based access control, least privilege, or separation of duties), security training, application security, monitoring, and governance. For example, for every sprint or new code release, our Security team conducts static code analysis, and for each major release, we perform manual penetration testing. The team also provides regular status updates to CDPH's Security and Privacy teams. Security is the responsibility of every team member, and we train our team on information security and project-specific security. Our Security team coordinates with CalVax's Program team for specific information security training and sends out regular security reminders. Our Security team also provides annual training to Vaccine Management Help Desk team members and to any new Help Desk team members within one week of joining the program.

With a strong focus on access control, we coordinate with the Help Desk team to document detailed processes for onboarding users, handling access change requests, offboarding users, and other requests. Accenture documents an access control policy that aligns with CDPH's security policy, plus a user access matrix and user access flow diagrams. We use role-based access control (RBAC) to make sure each user has only the least amount of privilege needed to perform their job function. We conduct

access control reviews for all Accenture team members quarterly, which are approved by the team members' supervisors. Additional user reports and reviews are conducted regularly for all users and require multi-factor authentication for all users, for all systems, unless otherwise approved by CDPH. Where possible, we use single sign-on (SSO) and virtual private networks. Accenture's security team is also available to help troubleshoot security-related issues with the various teams and users.

Vulnerability and patch management

Our security program entails continuous vulnerability and patch management activities such as conducting vulnerability scans, URL scans for certificate issues and security issues, endpoint patching with latest operating system, and security patching. The Endpoint team uses hardened OS and supports up to 50 servers for CalVax. The team coordinates with CDPH and CDT to manage certificates for the system, review threat intelligence, assess the latest attacks or vulnerabilities, and produce corrective action and mitigation plans for the Development team scheduled according to the severity of the vulnerability.

To harden the network and improve its security posture, we use an intrusion detection system (IDS)/intrusion prevention system (IPS) with CDPH. Our Security team reviews files for security concerns and produces corrective action plans/mitigations to be addressed based on the severity of the vulnerability identified. We follow Akamai configuration best practices to align with CDPH's security requests. We review the current configurations and provide status updates to CDPH security. The team configures AWS CloudFront firewall for endpoints, services, and applications where required and reviews configurations and changes. We support the use of Google ReCAPTCHA to prevent and detect bot attack attempts. We also evaluate and prepare to enact CDPH-approved Salesforce security recommendations and requirements to create the schedule. We use leading practices and Accenture's AWS configuration standards to protect containers, endpoints, and other services in the AWS environment.

Security monitoring

Our security monitoring includes supporting access control, reviewing alerts, and coordinating with the CDPH Security team for Microsoft Cloud Access Security (MCAS), Microsoft Defender for Cloud Applications, Extended Detection and Response (XDR), AWS security tools (like GuardDuty, Trusted Advisor, or Security Hub), and additional products as prescribed by the CDPH Security team. When changes to the system are required, we translate security findings into user stories and security-related components into accessible plain language. This helps the CDPH program staff understand the risks, user impact, and priorities for resolution. If needed, our Security team conducts meetings with development and CDPH program staff to explain the risks associated with each finding and steps for implementing the change.

Security incident management

For security incident management, we document an incident response guide, incident reporting template, notification process, and communication plan. If a security incident occurs, our team will notify CDPH Security and Privacy teams and begin coordination with all required teams. We provide regular investigation updates in the form of incident reports or in accordance with CDPH's prescribed notification process. We provide support for system availability concerns and assessing outages that may be the result of a security attack. If requested by CDPH, we conduct fraud investigations on a case-by-case basis. These fraud

investigations include documenting user activity, reviewing audit logs, generating application reports, completing a detailed report, and presenting the findings.

Maintenance

The CalVax System is available and accessible 24/7/365, except for scheduled downtime. The CalVax System is architected to be available when CalVax nightly batches are running. Requests to approve scheduled downtime go through the CalVax Project's Tech CAB process. The goal is to do as much planning upfront and provide as much lead time as possible to notify the counties of scheduled downtime. Accenture provides a tightly integrated organization to support CalVax and oversees the following functions as the prime vendor:

- **Infrastructure operations:** Environment management, capacity management, performance tuning, monitoring and error handling, patching and upgrades, and asset and configuration management
- **Application operations:** Batch operations, documentation and runbooks and integration with State, agency, or external interface partners/systems along with incident, problem, and defect management
- **Security:** Audits, disaster recovery, business continuity, security monitoring and error handling, and security incident management

Since December 2020, Accenture has demonstrated expertise with implementation, maintenance, and operation of the following technologies for CalVax:

- Oracle database and middleware products
 - Oracle Database Enterprise Edition - 19c
 - Oracle WebLogic Server - 12.2.1.4.0
 - Oracle JDK and JVM - Java 1.8.0.333
 - Oracle Enterprise Manager
- Adobe Experience Manager (SaaS)
- Windows Servers: Windows Server 2016/2019
- BICsuite Professional
- Informatica 10.2 to provide person data search capabilities

Interoperability

For the CDPH, the service desk level 3 support, the resolver groups were set up in the system to quickly dispatch tickets and resolve incidents. Accenture used MuleSoft to connect the system with other State and federal systems. We integrated the Salesforce system with several external systems including the State's Disease Surveillance System, multiple local health jurisdictions using API calls, CAIR2 for vaccination history, a SQL Server database system for auditing, a Snowflake system for reporting and

analytics, an AWS system that handles virtual agent interaction with residents, and more. The integration to the CAIR2 system is a real-time call from the Salesforce system to check the vaccination history of an individual per the request of a contact tracer working in Salesforce.

In addition, the service desk teams ensure that interoperability incidents across platforms are mapped to the correct team. The Tier 1, 2, and 3 teams interact daily to troubleshoot, triage, and resolve tickets.

Project #6	Contact #6
Company Name: State of Texas, Health and Human Services Commission (HHSC)	Contact Name: [REDACTED]
Project Name: Texas Medicaid and Healthcare Partnership (TMHP)	Contact Title: [REDACTED] [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) February, 28, 2003 through August, 31, 2023 Transition: February, 2003 through January, 2004 In production: January, 2004 through present	Address: [REDACTED] [REDACTED]
Contract Duration (months): 246 months	Phone Number: [REDACTED]
Contract Amount: More than \$2,000,000,000	Email: [REDACTED]
Describe the services provided:	

EXPERIENCE SUMMARY

As of January 4, 2023, Accenture has over 19 years of experience providing service desk activities on TMHP, a system that meets the definition of a large and complex IT system. As of January 4, 2023, Accenture has 19 years of experience performing service/help desk at TMHP. Service desk activities are currently ongoing through August 31, 2023. Therefore, our experience on TMHP **exceeds the requirement** as one of the two projects needed for F3.

PROJECT DESCRIPTION

In 2003, the Texas Health and Human Services Commission (HHSC), the single state agency charged with administration and oversight of the Texas Medicaid program, selected a partnership of contractors to take over the Texas Medicaid Management Information System (TMMIS) and Fiscal Agent services contract, establishing the Texas Medicaid and Healthcare Partnership

(TMHP). TMHP is a group of contractors under the leadership of Accenture. Accenture administers Texas Medicaid and other state health-care programs on behalf of the Texas Health and Human Services Commission. TMHP is responsible for administering Medicaid provider enrollment and fee-for-service claims processing for the State of Texas' Medicaid program. All Medicaid providers, both fee-for-service and managed care, must enroll through the TMHP for credentialing and licensing prior to authorization as a Medicaid provider. TMHP is also responsible for processing Medical Necessity and Level of Care (MN/LOC) Assessments for waivers. TMHP does not process claims for services provided by Medicaid managed care organizations (MCOs) but does collect encounter data from MCOs for use in evaluation of quality and utilization of managed care services.

For more than 19 years, Texas HHSC has been dedicated to delivering cost-effective, customer-focused health benefit programs for Texans through a commitment of continuous improvement, innovation, pragmatic technical solutions, and operational excellence. The TMHP supports fulfillment of the HHSC's business objectives and commitments.

Technical solution

Texas Medicaid is the third largest Medicaid program in the country, serving more than five million Texans and more than 120,000 health care providers, processing more than \$2 billion in annual payments for fee-or-service claims (Accenture does not issue capitation payments to managed care organizations). The TMMIS includes 42 subsystems and 14 primary business functions, including more than 800 staff and contractors, 22 subcontractor agreements, and nearly 70 contractors.

Services delivered

Accenture administers Texas Medicaid and other state health-care programs on behalf of the Texas Health and Human Services Commission and supports the TMMIS and Fiscal Agent services contract. Between 2003 and 2014, Accenture was the technology service provider for the TMMIS. In 2014, Accenture was brought in as the prime contractor in an emergency procurement. The BPO operations scope transitioned from the previous contractor to Accenture in 88 days with no down time. Accenture completed the operations takeover on time and under budget, and transitioned all Fiscal Agent operations, including support, maintenance, enhancements, project management, hardware and software management, and operation of components of the TMMIS.

As the prime maintenance and operations (M&O) contractor, Accenture is responsible for enhancing and operating the TMMIS, which includes supporting case and provider management applications, interfaces/integration points, and data center operations. Accenture maintains and/or modifies applications used in claims processing, provider management, contact center, federal reporting, and other MMIS functional requirements. Additionally, Accenture is responsible for TMMIS support scope, which includes systems planning, design, architecture, development, testing, implementation, operations coordination, and maintenance for healthcare automated systems and business application software that integrate hardware, software, and communication technology. This involves innovative solutions and advanced technologies, governance, and requirements gathering and development for complex, mission-critical systems. Accenture also provides full lifecycle system development, maintenance, and support services for one of the largest data warehouses in Texas state government. Accenture is currently

responsible for application maintenance, system modifications, system engineering, capacity planning, performance testing, performance monitoring, and batch processing for the current contract through August 2023.

Accenture has over 19 years of experience performing service/help desk activities using Information Technology Infrastructure Library (ITIL) standards and framework, supporting Tiers 1, 2, and 3 support, security, maintenance, and interoperability. Accenture has also established eligibility as a service for HHSC. The system has real-time interfacing which allows our trading partners to get eligibility data from the system real time, in batch and in an interactive manner.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The TMMIS integrates with Microsoft Dynamics CRM, Tableau, SAS, Blue Prism RPA, Avaya, and Business Objects. All of these are COTS applications.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The TMMIS processes over 1,400 outbound interfaces across 40 applications, with over 1,000 application endpoints. The Long-Term Care Online Portal has multiple real-time interfaces with other state of Texas HHS systems to exchange Medicaid provider, client, and service information. These interfaces use an electronic data interchange (EDI) system that contains real time interface transactions with external Medicaid providers for the receipts and response for claims and Medicaid eligibility information. The EDI system processes over 4 billion transactions per year.
3. **Is accessed by at least 1,000 users at multiple locations:** The TMMIS supports multiple web-based applications that are accessed by over 10,000 users at multiple locations each day in support of the Medicaid claims function. The system is also accessed by hundreds of state staff on a weekly basis. Some of the most-used systems include TexMed Connect, which enables the Medicaid provider community to conduct a variety of critical business transactions such as searching for client eligibility and submitting electronic claims, and Prior Authorization, which is also widely used on the portal.
4. **Has a contract value of at least \$10,000,000 dollars:** The TMHP contract value is more than \$2 billion.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** All our web-based applications use a three-tiered process: web layer, application layer, and database layers. Applications are available via web browser and are mobile compatible.

I-F3 EXPERIENCE DETAILS

Accenture has been performing service desk activities for TMHP since 2014. These activities include using ITIL standards and framework, supporting Tiers 1, 2, and 3, security, maintenance, and interoperability.

Service Desk experience, including supporting Tiers 1 and 2 service desks/help desks

At TMHP, we provide a fully operational service desk. It is based on a multi-tier service desk model, organized into three tiers: Tier 1, 2 and 3. Each tier of the model works as follows:

- Tier 1 is the initial contact and triage point for interactions with the Service Desk. Tier 1 will create cases for each interaction, triage, categorize the case, attempt to resolve and, if necessary, escalate to Tier 2 with the creation of a related Incident.
- Tier 2 handles incidents not resolved at Tier 1. Tier 2 attempts to answer functional and basic technical incidents. Upon resolution, the incident and related case(s) are all closed. For incidents that cannot be resolved by Tier 2, Tier 2 will escalate to Tier 3 for resolution.
- Tier 3 is staffed with our infrastructure, application development, production operations and technical subject matter experts. Tier 3 assigns incidents to the appropriate expert for application fixes or workarounds. Upon resolution, the problem and related incident(s) and case(s) are all closed after follow-up with caller to assure closure.

The TMHP ticketing system passes through various layers for resolution. This service desk model ensures end-users are provided the level of support to accelerate resolution.

As part of providing management of infrastructure operations, Accenture's services include:

- Patching of various hardware and software components
- Performing vulnerability scanning
- Updating antivirus daily
- Executing technical changes
- Managing Change Advisory Board and change request process
- Monitoring the infrastructure components for errors
- Error handling and corrective actions
- Supporting auditing solution and reporting
- Performance monitoring and tuning
- Creating runbooks and job aids
- Capacity management and reporting
- Managing user access
- Asset and configuration management

Using ITIL standards and framework

At TMHP, we employ the ITIL standards and framework. This provides a cohesive set of best practices, drawn from the public and private sectors internationally as the most widely accepted approach to IT service management in the world. Accenture Delivery Methods has incorporated ITIL best practices and terminology, with ITIL as the foundation for our Infrastructure Consulting methods. Accenture has thousands of individuals trained in ITIL and has been actively involved with the IT Service Management Forum, the ITIL user group, and the Office of Government Commerce (OGC) as the owner of ITIL. Alongside Carnegie Mellon University, Accenture is a co-author of the Service Strategies book, one of the five volumes in ITIL v3.

ISO 20000 (previously published as BS15000) is an international standard for IT Service Management based on ITIL. While ISO 20000 defines the requirements for service providers to plan for and deliver managed services, it also represents an industry consensus to help prepare for audits against ISO 20000. Accenture has achieved the ISO 20000 certification in multiple locations. The use of ITIL on the TMHP account promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements.

Security

The service desk is alerted when security incidents are detected. The Security Operation Center (SOC) will receive a ticket/notification to investigate the incident of a potential breach. Once they have completed their investigation and remedy the security-related issue, they notify the service desk, and the ticket is closed. Examples of security related incidents include unusual behavior of privileged user accounts; unauthorized insiders trying to access servers and data; phishing anomalies in network traffic; excessive consumption of server memory; unauthorized changes in configuration and unexpected account lockouts and password changes. The service desk works in collaboration with the SOC to ensure all aspects of security are communicated and resolved across the ecosystem.

A comprehensive security program providing confidentiality, integrity, and availability is critical to TMHP. All contract and security requirements are outlined in the responsibility traceability matrix. We also constructed a RACI matrix to eliminate gaps in security coverage. Accenture's security program complies with CDPH policies and standards, federal laws, local laws and regulations, and Accenture's policies. We have a Client Data Protection (CDP) program with controls to protect security and privacy that includes controls that must be validated regularly by our key staff.

Maintenance

The TMHP System is available and accessible 24 hours a day, 7 days a week, and 365 days a year, except for scheduled downtime. The TMHP System is architected to be up when the TMHP nightly batch is running. Requests to approve scheduled downtime will go through the project's Change Advisory Board (CAB) process. Prior to scheduled downtime, diligent planning activities are completed to provide a greater lead time and minimize the actual scheduled downtime. During regular scheduled maintenance, the Service Desk works with the teams to ensure that any issues are proactively provided and broadcast during calls and communication channels.

Accenture provides a tightly integrated infrastructure organization to support TMHP and is responsible for the following functions as the prime infrastructure contractor:

- **Infrastructure Operations:** Environment management, capacity management, performance tuning, monitoring and error handling, patching and upgrades, and asset and configuration management
- **Application Operations:** Batch operations, documentation and runbooks, integration with state, agency or external interface partners/systems, incident/problem, and defect management
- **Service Desk:** A multi-tiered service desk; Accenture is responsible for TMHP's service desk
- **Security:** Auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management

Accenture has demonstrated expertise with implementation, maintenance, and operation of over 40 production systems for TMHP. These TMHP solutions have many batch and real-time interfaces. For example, TMHP has real-time interfacing with trading partners to consume, allowing them to get eligibility data in an interactive manner.

Interoperability

The Service Desk works closely with the Tier 3 resolver teams for ticket resolution. As interoperability affects every part of TMHP, our work to support the infrastructure for interoperability has been similarly broad. Interoperability activities enable TMHP to work with other systems or products to exchange data or information. For our infrastructure team, interoperability is paramount as it enables TMHP to exchange data and information with external systems, products, and data sources. Increasing use of standards-based APIs has created the need for the infrastructure team to manage interoperability challenges and coordination with external applications. Collaboration and communication with the third parties with which we interoperate is critical. With better communication and collaboration, we help maintain interoperability over time.

Minimum Experience I-F4

Prime Contractor experience with a minimum of one (1) large and complex IT System Project involving your firm and a minimum of two additional contractors with responsibility for different areas of the system. The Project(s) must have been completed or ongoing within the last ten (10) years.

Project #1	Contact #1
Company Name: California Statewide Automated Welfare System (CalSAWS) Consortium	Contact Name: [REDACTED]
Project Name: California Statewide Automated Welfare System (CalSAWS)	Contact Title: [REDACTED]

(prior project name was the LEADER Replacement System (LRS), which is now called CalSAWS)	
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) LRS/CalSAWS November, 7, 2017 through April, 30, 2025	Address: [REDACTED] [REDACTED]
Contract Duration (months): 149 months	Phone Number: [REDACTED]
Contract Amount: LRS/CalSAWS \$1,425,495,842	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>At CalSAWS, a large and complex IT system, Accenture is the prime contractor with experience interacting with six additional contractors responsible for different areas of the system. The project is ongoing and therefore, our experience on CalSAWS alone exceeds the requirement stated in F4.</p> <p>PROJECT DESCRIPTION</p> <p>CalSAWS is an integrated eligibility system built and operated by the CalSAWS Consortium on behalf of the 58 counties of California. CalSAWS supports the counties in administering public assistance programs in California, including cash assistance (CalWORKs/TANF), food assistance (CalFresh/SNAP), medical assistance (Medi-Cal/Medicaid), and other state and county-specific programs.</p> <p>Technical solution</p> <p>CalSAWS is the most extensive integrated eligibility system in the United States and is hosted in the Amazon Web Services (AWS) cloud. Supporting over 10 million transactions daily, it has more than 50 interfaces, six of which are real-time. The system is currently in production in 42 counties. 18,500 users use this system daily across 125 locations to support 11 million Californians who receive public assistance. CalSAWS issues more than \$1 billion in benefits each month. By October 2023, all 58 counties will have migrated on to this platform. After all counties are migrated to CalSAWS, 41,000 internal users will use CalSAWS daily to support nearly 19 million Californians and issue nearly \$2 billion in benefits each month.</p> <p>Services delivered</p> <p>Accenture is one of six contractors responsible for CalSAWS and has the largest scope of work. Accenture's contract began in November 2012 and is ongoing through April 2025. As the prime contractor for systems integration and maintenance and operations (M&O), Accenture is responsible for application maintenance and system enhancements, and cloud-based operations including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing and</p>	

monitoring, and batch processing. Accenture supports hardware and software management, system engineering, data conversion, and project management. Accenture also supports the service desk (tiers 1, 2 and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework.

Accenture is responsible for the core CalSAWS eligibility system, the analytics application, ForgeRock identity solution, contact center technologies, the Child Care Provider Portal, and kiosks/tablets in several county lobbies. The CalSAWS Consortium has separate prime contracts for the legacy system maintenance (CalWIN), cloud hosting, public portal (BenefitsCal), imaging (SaaS contract), and print services.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CalSAWS solution integrates custom Java code with COTS applications (e.g., Oracle database and middleware products, Informatica Identity Resolution, Pitney Bowes Spectrum, ForgeRock, and IBM Operational Decision Manager). The core eligibility application further integrates with other COTS applications (e.g., Adobe Experience Manager and AWS Connect) and custom applications (e.g., OCAT, Child Care Portal, and BenefitsCal).
2. **Interfaces with at least five external systems, at least one of which is real-time:** The CalSAWS solution interfaces and exchanges with 50 external systems. BenefitsCal, CalHEERS, County Master Data Management (MDM), Lobby Monitors, the Online CalWORKS Appraisal Tool (OCAT), and Statewide Client Index all interface in real time.
3. **Is accessed by at least 1,000 users at multiple locations:** The CalSAWS solution is accessed by an average of 18,500 daily users across 125 locations. After the CalWIN counties are migrated, the number of CalSAWS users will be approximately 41,500.
4. **Has a contract value of at least \$10,000,000 dollars:** The CalSAWS contract value is \$1,425,495,842.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The CalSAWS core eligibility application includes a multi-tiered processing architecture, a presentation tier optimized for multiple user interface platforms (e.g., Google Chrome and Microsoft Edge), an application tier, and a data tier. Other components of the system run on other user interface platforms such as kiosks and tablets.

I-F4 EXPERIENCE DETAILS

The CalSAWS project includes Accenture and six other CalSAWS contractors responsible for different areas of the system. The Consortium monitors and oversees the work of all CalSAWS contractors for the DD&I and M&O phases of the CalSAWS Project. The Consortium acts as the liaison between stakeholders such as state and federal program sponsors, the JPA Board of Directors, Project Steering Committee, counties, interface partners, and advocates. The Accenture Project team currently provides M&O services as defined in the M&O Services Plan during the DD&I and M&O phases of the CalSAWS Project. The Accenture Project team oversees and performs the management, operations, maintenance, and enhancements for CalSAWS.

Accenture's interaction with other contractors includes the following:

1. **AWS:** AWS provides M&O services as defined in the CalSAWS AWS Agreement during the M&O phases of the CalSAWS Project. AWS provides and maintains the AWS cloud-hosted architecture and performs hosting services for the CalSAWS application. Accenture and AWS are in constant communication and collaboration. The Accenture/AWS strategic relationship is one of the strongest and most powerful in the industry today. Accenture has worked through challenging incidents and significant successes on CalSAWS, from storage constraints to improved batch mass changes requiring just 10% of the time the legacy system (LRS) required. AWS and Accenture are the largest and most influential actors in our industries—together, Accenture and AWS are a premier partnership for CalSAWS, the largest and most influential integrated eligibility system in the United States.
2. **Hyland Software:** The Hyland Software Project team provides M&O Imaging services as defined in the CalSAWS Accenture Amended, Restated, and Revised LRS Agreement, Exhibit Z (Statement of Services for CalSAWS Imaging Project) during the DD&I and M&O Phases of the CalSAWS Project. The Hyland Project team oversees and performs the management and operations of the AWS cloud-hosted Hyland Imaging Solution. Accenture, working collaboratively with the Consortium, Hyland, and other impacted contractors, led and facilitated the expansion of the Hyland SaaS offering to meet the CalSAWS performance requirements after the C-IV Counties went live on CalSAWS in October 2021.
3. **EY (formerly Cambria):** The EY (formerly Cambria) Project team provides M&O services as defined in the OCAT Agreement during the DD&I and M&O phases of the CalSAWS Project. The EY Project team oversees and performs the management, operations, maintenance, and enhancements for the OCAT application. Accenture collaborated with EY and several other contractors to develop the interfaces between OCAT and CalSAWS.
4. **Gainwell:** The Gainwell Project team provides M&O services as defined in the CalSAWS Central Print Services Agreement during the DD&I and M&O phases of the CalSAWS Project. The Gainwell Project team provides the technical services necessary to support the General Assistance/General Relief (GA/GR) correspondence and oversees and performs the management, operations, and delivery of Central Print Services, including planning, designing, managing, and operating the primary and backup print facility sites. For both Central Print and GA/GR, Accenture worked with Gainwell to assist them in their services to CalSAWS. Gainwell won the Central Print procurement (Accenture did not bid) and Accenture facilitated the seamless transition of print services. Regarding GA/GR, Accenture led the design and implementation efforts, coordinating with Gainwell over a period of more than two years to extract the necessary information to successfully automate the CalWIN GA/GR rules into CalSAWS.
5. **Deloitte:** The Deloitte Project team provides M&O services as defined in the CalSAWS Statewide Portal/Mobile (BenefitsCal) SOW during the DD&I and M&O phases of the CalSAWS Project. The Deloitte Project team oversees and performs the management, operations, maintenance, and enhancements for the BenefitsCal application. Accenture worked closely with Deloitte as they joined the CalSAWS Project to assist them in becoming familiar with the CalSAWS culture and environments.

Throughout the development of BenefitsCal APIs, Accenture collaborated closely with the Deloitte team to review, develop, and test the APIs to confirm they were performant.

6. **ClearBest:** The ClearBest Project team provides QA services as defined in the CalSAWS QA Services Agreement during the DD&I and M&O phases of CalSAWS. Accenture and ClearBest have worked together as the Consortium's primary contractor-partners, ensuring open and transparent communication so ClearBest could perform their QA responsibilities.

Accenture has been working with the CalSAWS Consortium for over two decades. We were the prime system integrator for C-IV, LRS, and CalSAWS. Accenture currently serves as the prime M&O contractor for the CalSAWS system and prime system integrator for migrating the remaining 16 counties. Accenture's duties span Infrastructure and M&E. As part of the CalSAWS DD&I project, Accenture is nearing completion of the migration of the Consortium's projects (C-IV, LRS M&O Project, CalSAWS M&O Project, CalWIN Project) into a single, seamless, AWS cloud-based solution.

Project #2	Contact #2
Company Name: State of Ohio, Department of Administrative Services (DAS)	Contact Name: [REDACTED]
Project Name: Ohio Benefits	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) February, 20, 2013 through June, 30, 2023	Address: [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 124 months	Phone Number: [REDACTED]
Contract Amount: \$530,000,000	Email: [REDACTED]

Describe the services provided:

EXPERIENCE SUMMARY

At Ohio Benefits, a large and complex IT system, Accenture is the prime contractor, with experience interacting with three additional contractors responsible for different areas of the system, and therefore our experience on Ohio Benefits **exceeds the requirement** stated in F4.

PROJECT DESCRIPTION

The Ohio Benefits program is a mature enterprise system that streamlines health and human services program delivery through standardized business processes which improve client outcomes. Ohio Benefits was initiated in 2012 to transform Ohio's enterprise integrated eligibility and health and human services system. It was designed to replace the 30-year-old Client Registry Information System, Enhanced (CRIS-E). The primary function of CRIS-E was benefit eligibility determination for beneficiaries of the Ohio Department of Job and Family Services (ODJFS) and Ohio Department of Medicaid (ODM) programs.

Ohio Benefits first went live in October 2013, and currently supports eligibility determination and benefit distribution for the State's Medicaid (including CHIP), SNAP (including P-EBT), Cash (including Temporary Assistance for Needy Families (TANF) and Refugee Cash Assistance), and Child Care programs. Ohio Benefits supports over 3 million residents and is used by over 10,000 county users across multiple locations in 88 counties.

Technical solution

Ohio Benefits integrates multiple COTS products including the Accenture Public Service Platform, IBM Cognos, Informatica Master Data Management, Adobe Experience Manager, and Tableau. Accenture implemented and supported Ohio Benefits with an innovative and scalable infrastructure designed for high availability, stability, and performance using Oracle's Private Cloud platform. Accenture implemented Oracle Linux virtual servers, Oracle databases, a series of Oracle Middleware products, and other software on this platform. Over time, Accenture implemented five key portals for the program: Citizen Self-Service Portal, Worker Portal, Provider Portal, Presumptive Eligibility/Deemed Newborn Portal, and Business Intelligence (BI) Portal.

The system supports integration with 47 state, agency, and other external interface partners and systems, including approximately 85 data exchanges (both real-time web services and file-based transfers). Interface partners include federal agencies such as the SSA, CMS, DHS, and IRS. Seven million real-time transactions are exchanged each month with various interface partners.

Benefit issuance data is transmitted to SNAP and Cash issuance contractors to deliver more than \$2.25 billion in annual SNAP payments, more than \$180 million in annual Cash payments, and over \$1 billion in P-EBT benefits since the beginning of the COVID-19 public health emergency. Real-time data is exchanged with the State's MMIS system, MITs, to support Medicaid service delivery for more than 3 million Ohioans. The system is architected for multi-tiered processing, including a user-facing front end designed to adapt to multiple user interface platforms (e.g., laptops, phones, and tablets).

Services delivered

In February 2013, Accenture was awarded the contract for Design, Development, and Implementation (DDI) for implementing the Medicaid, SNAP, TANF, and Child Care programs into Ohio Benefits and subsequent M&O services to support the administration of programs in the production environment. Accenture has served as the prime contractor for this project since inception, and the current contract ends in June 2023.

Accenture's infrastructure support for Ohio Benefits includes operations, performance testing, performance monitoring, security, network engineering, cybersecurity vulnerability testing and mitigation, capacity planning, and managing hardware and software. Accenture's application M&O support includes application maintenance, system modifications, system engineering, capacity planning, performance testing, performance monitoring, batch processing, data conversion, and project management.

Accenture also supports the Ohio Benefits solution via a multi-tier service desk (tiers 1, 2, and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework. Accenture is responsible for all phases of the enhancement software development lifecycle, including Analysis, Design, Development (Build) and Test, User Acceptance, Deployment, and Post-Deployment.

Accenture partners with multiple contractors on the program, including Deloitte for organizational change management services, Northwoods for electronic document management services, and Cincinnati Bell (CBTS) for computer telephony integration and interactive voice response services.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** Ohio Benefits is based on multiple COTS products including the Accenture Public Service Platform, IBM Cognos, Informatica Master Data Management, Adobe Experience Manager, and Tableau. Ohio Benefits runs on dedicated infrastructure leveraging Oracle's private-cloud platform: Oracle Exadata systems, Oracle Private Cloud Appliances, and Oracle ZFS storage, along with other third-party hardware security and operations components such as Micro Focus ArcSight and Veritas NetBackup.
2. **Interfaces with at least five external systems, at least one of which is real-time:** Ohio Benefits implements 85+ interfaces across 47 partners, including both State and Federal partners, such as the IRS, SSA, Accuity (Asset Verification – real-time), Central Print, Ohio Department of Health and Human Services (public assistance reporting), and Ohio Department of Developmental Disabilities (waiver eligibility information), among other partners. Batch and real-time interfaces are implemented leveraging Axway API gateway.
3. **Is accessed by at least 1,000 users at multiple locations:** Ohio Benefits supports over three million residents, and over 120,000 users access it across multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The Ohio Benefits contract value is over \$530 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** Ohio Benefits includes multi-tiered processing with a mobile-friendly, customer-facing front end for Self Service Portal (SSP) for Ohio residents.

I-F4 EXPERIENCE DETAILS

Ohio Benefits includes Accenture and three other contractors responsible for different areas of the system. The contract is ongoing through June 30, 2023.


Minimum of two additional contractors with responsibility for different areas of the system

The Ohio Department of Administrative Services (DAS) monitors and oversees the work of all Ohio Benefits contractors during all phases of the project. DAS acts as the liaison between multiple stakeholders, including Accenture and the three other Ohio Benefits IE system contractors. The responsibilities of the various system contractors include:

- **Accenture:** The project team currently provides services including security, helpdesk, application maintenance, system modifications, system engineering, capacity planning, performance testing, performance monitoring, batch processing, data conversion, infrastructure, and project management. Accenture interacts with all other contractors regularly.
- **Northwoods:** Responsible for the Enterprise Document Management System (EDMS). Accenture built and continues to maintain the interfaces with this partner.
- **CBTS:** Responsible for the IVR solution and telecom contractor. Accenture built and continues to maintain interfaces with this partner. Accenture also directly managed the co-location relationship with CBTS from 2013 through 2020, when the state decided to move to a consolidated space under a separate state contract.
- **Deloitte:** Responsible for organizational change management (OCM).

Our multi-contractor approach is focused on centralized governance, open communications, aligning cultures, and proven methods that bring contractors together as one team. We work with the Ohio Benefits Program PMO, project management, and the operations teams to provide a single point of management and consistent processes across organizations.

Project #3	Contact #3
Company Name: Centers for Medicare and Medicaid Services (CMS)	Contact Name: [REDACTED]
Project Name: HealthCare.gov/Federally Facilitated Marketplace (FFM) (including FFM, FFM Bridge and FFE)	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) January, 11, 2014 through January 10, 2027	Address: [REDACTED] [REDACTED]
Contract Duration (months): 156 months	Phone Number: [REDACTED]

<p>Contract Amount: HHSM-500-2014-00191C: \$198,111,211 HHSM-500-2015-00246C: \$842,454,559 HHSM-500-2016-00003I/75FCMC21F0001: \$205,006,767 HHSM-500-2016-00003I/75FCMC21F0002: \$322,884,001 Total: \$1,363,449,771</p>	<p>Email: </p>
<p>Describe the services provided:</p> <p>EXPERIENCE SUMMARY</p> <p>At HealthCare.gov, a large and complex IT system, Accenture is the prime contractor working with more than four other contractors responsible for different areas of the system, as well as contractors in all 50 states, insurance companies, and the IRS. The contract is ongoing through January 10, 2027, and therefore our experience on HealthCare.gov exceeds the requirement stated in F4.</p> <p>PROJECT DESCRIPTION</p> <p>Through the 2010 Patient Protection and Affordable Care Act (ACA), new health insurance exchanges were created at both the state and federal levels. These exchanges are public-private marketplaces where Americans can securely shop for health insurance plans and apply for a tax subsidy simultaneously with multiple insurance companies. HealthCare.gov, the eligibility website for the federal exchange, is the front door for the Federally Facilitated Marketplace (FFM). Ancillary systems include FFM Bridge and Federally Facilitated Exchanges (FFE).</p> <p>Technical solution</p> <p>FFM is a cloud-based solution and uses a multi-tiered processing architecture, including a presentation tier optimized for multiple user interface platforms (such as laptops and mobile devices), an application tier, and a data tier. The system integrates with several COTS solutions (e.g., Salesforce and Interactive Voice Response (IVR)), which integrate with custom applications that are developed, deployed, and operated on Confluence and Red Hat software. The system was migrated to the Amazon Web Services (AWS) cloud platform in 2019 and has been running on that platform since then.</p> <p>FFM connects with over 800 issuers enabling data sharing and claims processing in the cloud in compliance with CMS analytical algorithms. A feature of the FFM system is its innovative way of adapting to meet the unique needs of each of the 50 states through interfaces with health insurance companies and the IRS. Some states use the system's full functionality, and others use the system solely for essential eligibility functions. FFM consists of seven subsystems and has real-time integration with external systems</p>	

(e.g., IRS, SSA, and DHS) to validate eligibility. FFM is utilized in multiple locations across the country annually by over 1,000 internal and 10 million external users to enroll in qualified health insurance plans.

Services delivered

A rescue of the website began in November 2013, and in January 2014, the federal government hired Accenture as the prime contractor for application maintenance, system modifications, cloud-based operations, project management, cybersecurity vulnerability mitigation, network and system engineering, capacity planning, performance testing and monitoring, and batch processing. In just six weeks, Accenture mobilized more than 500 skilled professionals to transition the system from the original vendor to Accenture at an unprecedented speed.

Working closely with the original vendor, Accenture quickly achieved CMS' objective to stabilize and enhance HealthCare.gov. A collaborative and comprehensive transition plan was created that mitigated the risk and enabled Accenture to begin hands-on delivery. Within eight weeks, Accenture delivered significant technical enhancements to the website, stabilizing it during the peak of HealthCare.gov's initial enrollment period. This enabled millions of Americans to securely enroll in health insurance.

Accenture is responsible for stabilizing, securing, and improving the website, maintaining hardware/software, and developing additional systems and interfaces while managing maintenance and operations. In addition to providing issuers with a complete data processing environment, Accenture developed an innovative solution that each issuer owns and operates. The FFM modernization projects for HealthCare.gov include Accenture as the prime contractor, four other vendors responsible for different areas of the system, contractors in all 50 states, insurance companies, and the IRS.

The FFM Service Desk, a multi-tier service desk, is managed and operated by Accenture in partnership with CMS. CMS is responsible for Tier 1 support. Accenture is responsible for Tier 2 and Tier 3 support using the Information Technology Infrastructure Library (ITIL) standards and framework. Additional support services include security, maintenance, and system interoperability. More than 50,000 issues were triaged and resolved by the FFM Service Desk between 2015 and 2022.

Accenture has successfully operated through seven open and special enrollment periods in collaboration with CMS and other FFM stakeholders to support 45 million enrollments and \$200 billion in total payments since 2015. Accenture's contract has been renewed three times and is ongoing through January 10, 2027.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** FFM consists of seven subsystems that interface with each other and integrate with external systems including COTS packages like Salesforce with custom-developed components built and deployed upon software by Confluence and Red Hat. FFM's seven subsystems include Eligibility and Enrollment, Stand-Alone Eligibility, Plan Management, Financial Management, Marketplace Consumer Record, Insurance Enrollment System and the Document Storage and Retrieval System.

2. **Interfaces with at least five external systems, at least one of which is real-time:** FFM interfaces with internal CMS components and systems external to CMS, including 27 state systems to support account transfers. FFM has real-time integrations with IRS, SSA, and DHS systems to validate eligibility via the CMS HUB. For issuer support, the System Exchange Enrollment Data application integrates with FFM. For eligibility support, the Eligibility Support system integrates with FFM for DMI/SVI adjudication. The Eligibility Support Desktop Change Utility Tool integrates with FFM to assist with appeals and eligibility determinations of consumers. The Next Generation Desktop integrates with the FFM for call center support. For issuer payment, it interacts with CMS' HIGLAS general ledger and payment system.
3. **Is accessed by at least 1,000 users at multiple locations:** FFM is used by over 1,000 internal users and 10 million consumers annually to enroll in qualified health insurance plans across 34 states.
4. **Has a contract value of at least \$10,000,000 dollars:** The FFM contract value is \$1.36 billion over 13 years.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The FFM solution includes multi-tiered processing, including online, API-based, and batch processing, with data integration for internal and external partners. FFM is highly tuned to support evolving consumer needs—the customer facing front-end is optimized for multiple user interface platforms. Accenture conducts significant performance testing and tuning in close collaboration with CMS to ensure FFM is aligned with CMS' objectives for each open enrollment period.

I-F4 EXPERIENCE DETAILS

As part of the FFM program, Accenture performs significant modernization projects involving multiple contractors. We identify four of these contractors and their responsibilities here. Accenture modernized the Marketplace Eligibility System and Marketplace Plan Management system, working in close coordination with the following contractors:

- **Sparksoft:** Supports the Marketplace Data Warehouse and Data Services Hub
- **SERCO:** Performed eligibility support
- **Logistics Management Institute (LMI):** Performs plan reviews
- **Impaq:** Supports interaction with QPH issuers

To varying degrees, we are involved with other contractors from all 50 states. This includes 27 states who rely fully on the FFM for its marketplace, seven states who use FFM but retain certain essential functionality for operating a marketplace, and the 16 states who operate their own State Based Marketplace (SBM) but still rely on HealthCare.gov to fulfill enrollment and eligibility functions. Additionally, we interface with the health insurance companies for enrollment, premium payment, and risk adjustment programs to support premium price stabilization and accurate payments and the IRS for tax subsidy purposes.

CMS recognized Accenture for consistently providing support to other contractors in the Marketplace ecosystem. CMS has formally recognized Accenture's role in helping other contractors through multiple CMS-approved "Notable Achievements."

Project #4	Contact #4
Company Name: U.S. Department of Treasury Internal Revenue Service	Contact Name: [REDACTED]
Project Name: Integrated Enterprise Portal (IEP) 1.5 Program	Contact Title: [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) IEP 1.0 May, 19, 2011 through May, 18, 2017 IEP 1.5 February, 15, 2017 through February, 14, 2025	Address: [REDACTED] [REDACTED] [REDACTED]
Contract Duration (months): 164 months	Phone Number: [REDACTED]
Contract Amount: Exceeds \$1 billion	Email: [REDACTED]

EXPERIENCE SUMMARY

For the Federal Treasury IEP, Accenture is the prime contractor, working with five other contractors responsible for different areas of the system. Federal Treasury IEP meets the criteria for a large and complex IT system project, and our contract is ongoing through February 14, 2025. Therefore, our experience on IEP **exceeds the requirement** stated in F4.

Project Description

The IEP 1.5 Program is the digital front door to the Internal Revenue Service's (IRS) backend systems and provides technology services to thousands of internal and external users. It is mission critical in securely serving taxpayers, tax preparers, and employees. By continuously improving and innovating its platforms and applications through the IEP 1.5 Program, the IRS is sustaining its infrastructure and applications, expanding capabilities, and increasing resiliency.

Initially transitioning two portals from another contractor, Accenture's involvement with the IEP began in May 2011 on the IEP 1.0 Program. In February 2017, Accenture partnered with the IRS on the IEP 1.5 Program to perform maintenance and operations of its infrastructure and applications.

Technical solution

A key component of the IEP 1.5 infrastructure is its ability to deliver a scalable, elastic infrastructure using cloud-based services. The IEP infrastructure is designed to support iterative transformation without service disruption. IEP 1.5 encompasses the following systems and domains:

- Public User Portal (PUP – IRS.gov)
- Registered User Portal (RUP)
- Employee User Portal (EUP)
- Portal Account Replacement Tool (PART)
- Affordable Care Act Transactional Portal Environment (ACA-TPE)
- Certified Professional Employer Organization (CPEO) & 501(c)(4) Online Registration System
- Field Assistance Scheduling Tool (FAST)
- 90+ managed applications
- 3,500+ servers

The IEP features a multi-tiered processing architecture, including three user portals optimized for multiple user interface platforms (e.g., laptops and mobile devices). As part of the IEP solution, Accenture integrated over 90 applications, including ServiceNow and CPEO Versa, both of which are COTS applications. Accenture has also integrated five external systems, including the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.

The modernized system is accessed by over 1,000 internal users from multiple locations. During the 2021 filing season (February 12 to May 17, 2021), there were 767.1 million total site visits (from internal and external users) to IRS.gov and 2.02 billion page views on the site. The peak day was March 15, 2021, when 37.3 million visited the site and 88.1 million pages were viewed.

Services delivered

As the prime contractor, Accenture uses AWS cloud services for production applications and manages more than 40 public applications. Accenture is responsible for system modifications, hardware/software, project management, and cloud-based operations activities such as network and system engineering, cybersecurity vulnerability mitigation, capacity planning, performance testing and monitoring, and batch processing. Accenture also supports security, maintenance, and interoperability. The large and complex Federal Treasury IEP Program contract value exceeds \$1 billion and is ongoing through February 2025.

Using the Information Technology Infrastructure Library (ITIL) as the service desk framework, Accenture provides Tier 1 and Tier 2 service desk support for the IEP non-production environments. The IEP service desk supports request fulfillment, incident

management, problem management, and asset management. Additionally, the IEP service desk provides initial support for all IEP-related incidents, including opening tickets in the ITSM system to coordinate with other IRS organizations for incidents outside of the IEP purview.

Accenture created the IRS.gov website Help Desk, which serves as a “first aid station” for IRS.gov website questions such as navigation of IRS content and forms retrieval. The IRS.gov website Help Desk is a complementary service to the IRS toll-free tax assistance line. Accenture successfully delivered the IRS.gov website Help Desk for the IRS for 15 years and acted as the front door for many IRS.gov website visitors in their interactions with IRS.

Accenture collaborates in a multi-contractor environment with five other contractors responsible for different areas of the IEP. Accenture works with contractors such as Leidos, Deloitte, and Booz Allen to manage and maintain the IRS' infrastructure and coordinate the five legislatively mandated applications currently under development in the IEP's AWS-managed service cloud (two of which are Accenture-managed). Accenture is currently migrating legislatively mandated applications to the cloud and is expected to complete the migration of the remaining applications by January 2023.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The IEP solution integrates with over 90 applications. ServiceNow and CPEO Versa are two of the top COTS applications. In addition, PART is a care act identity management COTS product and FAST is the ServiceNow COTS product.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The IEP solution interfaces with more than five external systems, hosted by Health and Human Services for Medicare & Medicaid Services (HHS CMS) and IRS back-end systems. The applications include but are not limited to the Affordable Care Act (ACA) Application-to-Application (A2A) Transactional Portal Environment, Modernized eFile (MeF), Secure Access Digital Identity (SADI), Online Account/WebApps, and eServices real-time. These applications support real-time data access for taxpayers and other transmitters.
3. **Is accessed by at least 1,000 users at multiple locations:** The IEP solution is accessed by more than 1,000 users at multiple locations. The PUP—the IRS external or internet portal, IRS.gov, that allows unrestricted public access to non-sensitive materials and applications had 2.02 billion page views and 767.1 million total visits during the 2021 filing season (February 12–May 17, 2021).
4. **Has a contract value of at least \$10,000,000 dollars:** The IEP solution contract value exceeds \$1 billion.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The IEP solution features multi-tiered processing, including a customer or user facing front-end optimized for multiple user interface platforms. There are three main portals: PUP, registered user portal, and employee user portal. The ACA Application-to-Application (A2A) is a core interface.

I-F4 EXPERIENCE DETAILS

Accenture collaborates with five (5) other contractors to manage and maintain the IRS' infrastructure and applications and coordinate the five legislatively mandated applications currently under development in the IEP managed service cloud hosted through AWS (two of which are Accenture-managed). Three of the additional contractors that provide support in other areas are Leidos, Deloitte and Booz Allen who support the mandated applications. One of these applications is developed by **Leidos**, one by **Deloitte**, and the third by **Booz Allen**. Deloitte also provides program management support for five of the applications. Accenture works in a multi-contractor ecosystem working in close collaboration with the contractors. For Treasury cloud, Accenture provides IaaS for another contractor. We also provide application and infrastructure support for at least five different application contractors and development support for more than 45 Registered User Portal (RUP) applications.

The IEP **Application Infrastructure Integration Services (AIIS)** is the support team that works with the IRS to help correctly configure IRS-owned applications to run on the IEP platform. IEP 1.5's AIIS team has a variety of responsibilities from performance tuning, application deployment, incident response and onboarding, configuration and troubleshooting, shared service support, and engineering services.

We also work collaboratively with the Modernized eFile (MeF) application team supported by a different contractor (**IBM**). MeF is the core web-based application that allows electronic filing of corporate, individual, partnership, exempt organization, and excise tax returns. For MeF, we provide the AIIS on the front end and interface with them for the backend data layer. In 2021, Accenture designed, built, and continues to maintain the IEP infrastructure components needed for the MeF Resiliency effort. Resiliency allows MeF components in the IEP to continue to accept submissions while backend services are unavailable.

Project #5	Contact #5
Company Name: State of California – California Department of Public Health (CDPH)	Contact Name: [REDACTED]
Project Name: California Vaccine Management Project (CalVax)	Contact Title: [REDACTED] [REDACTED] [REDACTED]
Contract Date(s): Start (Month, Day, Year) through End (Month, Day, Year) December, 14, 2020 through June, 30, 2023	Address: [REDACTED] [REDACTED]
Contract Duration (months): 30 months	Phone Number: [REDACTED]

Contract Amount: \$280,000,000	Email: [REDACTED]
Describe the services provided:	
<p>EXPERIENCE SUMMARY</p> <p>Accenture is the prime contractor at CalVax, a large and complex IT system, and interacts with four other contractors including Blue Cross/Blue Shield (BCBS), Maximus, Gainwell, and Lyniate who are responsible for different areas of the system. The project is ongoing through June 30, 2023, and, therefore, our experience on CalVax exceeds the requirement stated in F4.</p> <p>PROJECT DESCRIPTION</p> <p>The California Department of Public Health (CDPH) is a department of the Health and Human Services Agency of the Government of the State of California (the State). CDPH is responsible for public health across the State—setting policy and delivering services to California's 39 million citizens directly or through the State's 61 County or City Local Health Authorities. CDPH delivers services and oversees eligibility determination for a broad range of programs, including public health social services programs like the nutrition program for Women, Infants, and Children (WIC) and the Maternal, Child, and Adolescent Health program. In addition to its social services mandate, the CDPH is the agency charged with overseeing infectious disease control and prevention, leading the State's response to the COVID-19 pandemic.</p> <p>When COVID-19 vaccines finally became available, California public health officials not only wanted to get them to the public as soon as possible, they set an ambitious goal of aiming to immunize 70% of their 39 million residents within only six months. Accenture launched CalVax in December 2020, a large-scale system integration program to help the State reach this goal.</p> <p>Technical solution</p> <p>CalVAX operations is comprised of myCAvax, My Turn, and My Turn Volunteer. The CalVAX solution includes a multi-tiered architecture, including four front-end applications optimized for various user interface platforms. Accenture used MuleSoft as the strategic integration and application programming interface (API) platform. This integration connects with more than seven external systems to integrate the new Salesforce-based vaccine management system with other state and federal systems for the CDPH. Salesforce Lightning Flow Builder, a process automation tool that "calls" MuleSoft's API, is an example of real-time integration delivered by Accenture. The solution interacts with the California Immunization Registry (CAIR2), a COTS solution provided by Gainwell, in real-time to return the validity of healthcare providers. This enabled providers to register in the Salesforce system to order or administer vaccines. This real-time integration helps prevent unauthorized providers from accessing the system and streamlines the registration process that otherwise would require manual intervention.</p> <p>The My Turn website determines eligibility for vaccines and schedules over 625,000 appointments per month. The My Turn Volunteer website helped volunteers connect with the program to expedite the administration of vaccines. In total, over 10 million</p>	

vaccination appointments have been scheduled. The myCAVax solution alone supports 20,000 internal end users and 2,000,000 external users at multiple locations.

Services delivered

To support the statewide vaccination campaign, the CDPH joined forces with Accenture, the Federal Emergency Management Agency (FEMA), and Blue Shield of California to develop a secure, integrated vaccine management solution. Through this partnership, more than 50,000 vaccines were administered to residents every day throughout the pandemic. As the prime contractor, Accenture developed and oversaw CalVAX operations. Accenture managed multiple development teams working in parallel and delivered incremental product features to administer vaccinations as quickly as possible. Using the Agile software development life cycle (SDLC) approach, Accenture configured and launched these solutions in a matter of weeks, with additional critical functionality deployed every two weeks.

Throughout its contract period, Accenture has supported Tier 1, 2, and 3 service desk activities using the Information Technology Infrastructure Library (ITIL) standards and framework. As part of maintenance, Accenture provides a tightly integrated organization to support CalVAX and is responsible for infrastructure operations including environment management, capacity management, performance tuning, monitoring, and error handling, patching and upgrades, and asset and configuration management. Accenture also supports application operations such as batch operations, integration with state, agency or external interface partners/systems, and incident/problem and defect management. Security activities include auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management.

MEETING THE LARGE AND COMPLEX IT SYSTEM REQUIREMENTS

1. **Integrates with at least two applications, one of which is a COTS:** The CalVAX solution integrates with multiple state and federal systems including CAIR2, a COTS solution provided by Gainwell.
2. **Interfaces with at least five external systems, at least one of which is real-time:** For CDPH, we used MuleSoft to integrate the Salesforce-based contact tracing system with more than seven external systems. The included the state's Disease Surveillance system, multiple local health jurisdictions using API calls, CAIR2 for vaccination history, a SQL Server database system for auditing, a Snowflake system for reporting and analytics, an AWS system that handles virtual agent interaction with residents, and more. The integration to the CAIR2 system is a real-time call from the Salesforce system to check the vaccination history of an individual per the request of a contact tracer working in Salesforce.
3. **Is accessed by at least 1,000 users at multiple locations:** The myCAVax solution alone involves 20,000 internal end users and 2 million external users at multiple locations.
4. **Has a contract value of at least \$10,000,000 dollars:** The CalVax contract value is \$280 million.

I-F4 EXPERIENCE DETAILS

At CalVax, Accenture collaborates in a multi-contractor environment with BCBS, Maximus, Gainwell, and Lyniate for cloud-based areas including interfaces, data stores, software, services, migration, and mining.

Involving a minimum of two (2) contractors

The CDPH monitors and oversees the work of all CalVax contractors during all phases of the project. The Accenture Project team currently provides services as defined in the service plan. We oversee and perform the management duties, operations activities, application maintenance, and enhancements for CalVax. Accenture's multi-contractor relations on CalVax include the following vendors:

1. **Blue Cross/Blue Shield:** BCBS is the third-party administrator of the COVID-19 vaccine. Its role included determining the distribution of the vaccine across the providers and local health departments in California. Accenture and BCBS collaborated on various areas of policy and eligibility criteria as the vaccine rollout criteria evolved. Accenture and BCBS continuously worked together on the following activities:
 - Evolving eligibility criteria and support for the next wave of residents becoming eligible to receive the vaccine
 - Providing equal access methods to reserve vaccine appointments to for underserved populations
 - Advising CDPH and CDT on policy, vaccine distribution criteria, and third-party (off My Turn) vaccine appointment availability and data reporting requirements
 - Using predictive models for future vaccine distribution across the State based on My Turn data and socio-economic datasets
2. **Maximus:** Maximus operates and runs the resident-facing call center for COVID-19 vaccinations. Accenture was responsible for the provider and local health department call center for COVID-19 vaccine administration. Both call centers had an automated IVR flow that required coordination and handoffs between the two systems along with data reporting. Accenture and Maximus collaborated continuously on the following activities:
 - Designing and coordinating an IVR menu for cold and warm handoffs between systems
 - Sharing and coordinating call center scripts for warm handoff transitions
 - Testing IVR changes between systems to confirm IVR menu options continued to direct users to correct menu tree locations
 - Sharing and communicating call center reporting to determine health of the vaccine program and provide forward-looking predictions of call volume to properly size both help desks
3. **Gainwell:** Gainwell maintains and supports the CAIR2 system. CAIR2 is California's immunization registry where health providers across the State report patient immunization data. Accenture is responsible IRIS, a data warehouse sourcing data

from CAIR2 at near real-time frequency. The CAIR2 and IRIS systems are very tightly coupled. Accenture and Gainwell collaborate continuously on the following:

- Performing data migration and cutover for State Registry consolidation occurring between SDIR and CAIR2 (April 2022) and RIDE and CAIR2 (November 2022)
- Providing ongoing technical upgrades of the CAIR2 databases and corresponding IRIS system updates and adjustments
- Updating vaccination schedules in CAIR2 (Gainwell task) that are then migrated and synced into the IRIS data pipelines managed by Accenture with every change in vaccine eligibility and addition of new vaccination products
- Managing hourly monitoring of data extracts across CAIR2 and IRIS

- 4. Lyniate:** As part of its COVID Vaccine Management initiatives at the CDPH, Accenture needed to integrate the Vaccine Administration solution built on Salesforce (My Turn) with the State immunization registries to report patient COVID vaccinations within the State's 24-hour mandatory window. CDPH already had an integration tool in place called Lyniate Rhapsody. Rhapsody accepted immunization feeds to the registries from various providers, but there was no bi-directional automated exchange that operated at the scale of My Turn. This required careful collaboration with the Rhapsody contractor, Lyniate, to design, develop, test, deploy, and support a new integration solution. Accenture's MuleSoft team and the Lyniate team worked to establish a solid, reliable, and scalable bi-directional flow of data between My Turn and the State registries. This included troubleshooting issues during nights and weekends when needed and working together to identify areas for improvement. Ultimately, CDPH counted on our teams to make sure our platforms interacted effectively to serve residents' needs.

12.9 ATTACHMENT A9 – INFRASTRUCTURE FIRM REFERENCE FORM

Directions:

Provide two (2) Firm References for the Prime Contractor from the Projects listed in Attachment A8 – Infrastructure Firm Qualifications. Each Firm Reference must clearly identify the firm.

The Firm references must be submitted within the Business Proposal as defined within RFP Section 6 - Proposal Structure and Submission.

FIRM REFERENCE: ACCENTURE	
Reference Agency Name: State of California – California Department of Public Health (CDPH)	
Project Name: California Vaccine Management Project (CalVAX)	
Contact Person/Title: [REDACTED] [REDACTED] [REDACTED] [REDACTED]	Phone: [REDACTED]
Address: [REDACTED] [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project description</p> <p>The California Department of Public Health (CDPH) is a department of the Health and Human Services Agency of the State of California (the "State"). CDPH is responsible for public health across the State—setting policy and delivering services to California's 39 million residents directly through the State or the 61 County or City Local Health Authorities. CDPH delivers services and oversees eligibility determination for a broad range of Public Health Social Services programs such as the nutrition program for Women, Infants, and Children (WIC) and the Maternal, Child, and Adolescent Health program. In addition to its social services mandate, the CDPH is charged with overseeing infectious disease control and prevention, leading the State's response to the COVID-19 pandemic.</p> <p>When COVID-19 vaccines finally became available, California public health officials wanted to get them to Californians as soon as possible and set an ambitious goal of immunizing 70% of their 39 million residents within six months. CDPH contracted with Accenture in December 2020 to launch myCAvax, an innovative large-scale system integration program to help the State of California reach this goal.</p> <p>Technical solution</p> <p>CalVAX operations is comprised of myCAvax, MyTurn, and MyTurn Volunteer. The CalVAX solution includes a multi-tiered architecture, including four front-end applications optimized for various user interface platforms. Accenture used MuleSoft as the strategic integration and application programming interface (API) platform. This integration connects with more than</p>	

seven external systems to integrate the new Salesforce-based vaccine management system with other state and federal systems for the CDPH. Salesforce Lightning Flow Builder, a process automation tool that "calls" MuleSoft's API, is an example of real-time integration delivered by Accenture. The solution interacts with the California Immunization Registry (CAIR2), a COTS solution provided by Gainwell, in real-time to return the validity of healthcare providers.

The MyTurn website determines eligibility for vaccines and schedules over 625,000 appointments per month. The MyTurn Volunteer website helped volunteers connect with the program to expedite the administration of vaccines. In total, over 10 million vaccination appointments have been scheduled. The myCAVax solution alone supports **20,000 internal end users** and **2,000,000 external users** at multiple locations.

Accenture services delivered

To support the statewide vaccination campaign, the CDPH joined forces with Accenture, the Federal Emergency Management Agency (FEMA), and Blue Shield of California to develop a secure, integrated vaccine management solution. Through this partnership, more than 8,000 vaccines were administered to Californians every day throughout the pandemic. As the **prime contractor**, Accenture developed and oversaw CalVAX operations. Accenture managed multiple development teams working in parallel and delivered incremental product features to administer vaccinations as quickly as possible. Using the Agile software development life cycle (SDLC) approach, Accenture configured and launched these solutions in a matter of weeks, with additional critical functionality deployed every two weeks.

Throughout its contract period, Accenture has supported Tier 1, 2, and 3 **service desk activities** using the Information Technology Infrastructure Library (ITIL) standards and framework. As part of maintenance, Accenture provides a tightly integrated organization to support CalVAX and is responsible for infrastructure operations including environment management, capacity management, performance tuning, monitoring, and error handling, patching and upgrades, and asset and configuration management. Accenture also supports application operations such as batch operations, integration with state, agency or external interface partners/systems, and incident/problem and defect management. Security activities include auditing, disaster recovery and business continuity, security monitoring and error handling, and security incident management.

Accenture interacts with four other vendors—Blue Cross/Blue Shield, Maximus, Gainwell, and Lyniate—in a **multi-contractor environment** for cloud-based areas including interfaces, data stores, software, services, migration, and mining.

Accenture's **contract value of CalVAX is \$280 million** and the contract ends in June 2023.

Reference Questions: For each question below, please provide a comment.

1. Did the Contractor produce high quality deliverables? Please describe briefly.

Yes, the contractor delivered high quality deliverables under extreme time pressures. The contractor developed a vaccine management system for COVID that included ordering, enrollment, patient appointments, clinic management, and volunteer coordination.

2. Was the Contractor flexible and willing to work through issues during all stages of the Project?

Yes, the COVID response was extremely unpredictable and required that we pivot at a moments notice. Accenture was a dedicated partner and worked closely with us to meet all of the demands with unreasonable deadlines and under extreme pressure.

3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.

Yes, we were in close communication with all aspects of the project. Accenture was available at all hours, on weekends, and extremely responsive.

4. Were there any major issues with Key Staff turnover or replacement?

There were times where there was staff turnover during key times due to staff illness or burnout. Given the high demands, I suppose that is to be expected.

Reference Questions: For each question below, please provide a comment.

5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?

There were other partners such as Skedulo and Mulesoft. Accenture managed the tasks of these partners without issue.

6. Was the Project a success?

Yes, it is unbelievable that we were able to develop and launch new vaccine management systems during a pandemic. The systems weren't perfect when we launched them due to time constraints, but we worked diligently together to iterate and improve them every week.

7. Would you rehire/recommend this Contractor? If not, why not?

Yes, absolutely.

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?

10

Reference Questions: For each question below, please provide a comment.

Other Comments:

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name	██████████
Title	██████████
Date	██████████
Signature	██

FIRM REFERENCE: FIRM NAME	
Reference Agency Name: United States Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS)	
Project Name: HealthCare.gov/Federally Facilitated Marketplace (FFM)	
Contact Person/Title: [REDACTED]	Phone: [REDACTED]
Address: [REDACTED] [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project description</p> <p>Through the 2010 Patient Protection and Affordable Care Act (ACA), new health insurance exchanges were created at both the state and federal levels. These exchanges are public-private marketplaces where Americans can securely shop for health insurance plans and apply for a tax subsidy simultaneously with multiple insurance companies. HealthCare.gov, the eligibility website for the federal exchange, is the front door for the Federally Facilitated Marketplace (FFM). Ancillary systems include FFM Bridge and Federally Facilitated Exchanges (FFE).</p> <p>Technical solution</p> <p>FFM is a cloud-based solution and uses a multi-tiered processing architecture, including a presentation tier optimized for multiple user interface platforms (such as laptops and mobile devices), an application tier, and a data tier. The system integrates with several COTS solutions (e.g., Salesforce and Interactive Voice Response (IVR)), which integrate with custom applications (e.g., Java and Python) that are developed, deployed, and operated on Confluence and Red Hat software. The system was migrated to the Amazon Web Services (AWS) cloud platform in 2019 and has been running on that platform since then.</p> <p>FFM connects with over 800 issuers enabling data sharing and claims processing in the cloud in compliance with CMS analytical algorithms. A feature of the FFM system is its innovative way of adapting to meet the unique needs of each of the 50 states through interfaces with health insurance companies and the IRS. Some states use the system's full functionality, and others use the system solely for essential eligibility functions. FFM consists of seven subsystems and has real-time integration with external systems (e.g., IRS, SSA, and DHS) to validate eligibility. FFM is utilized in multiple locations across the country annually by over 1,000 internal and 10 million external users to enroll in qualified health insurance plans.</p> <p>Accenture services delivered:</p> <p>A rescue of the website began in November 2013, and in January 2014, the federal government hired Accenture as the prime contractor for application maintenance, system modifications, cloud-based operations, project management, cybersecurity vulnerability mitigation, network and system engineering, capacity planning, performance testing and monitoring, and batch processing. In just six weeks, Accenture mobilized more than 500 skilled</p>	

professionals to transition the system from the original vendor to Accenture at an unprecedented speed.

Working closely with the original vendor, Accenture quickly achieved CMS' objective to stabilize and enhance HealthCare.gov. A collaborative and comprehensive transition plan was created that mitigated the risk and enabled Accenture to begin hands-on delivery. Within eight weeks, Accenture delivered significant technical enhancements to the website, stabilizing it during the peak of HealthCare.gov's initial enrollment period. This enabled millions of Americans to securely enroll in health insurance.

Accenture is responsible for stabilizing, securing, and improving the website, maintaining hardware/software, and developing additional systems and interfaces while managing maintenance and operations. In addition to providing issuers with a complete data processing environment, Accenture developed an innovative solution that each issuer owns and operates. The FFM modernization projects for HealthCare.gov include Accenture as the prime contractor, more than six other vendors responsible for different areas of the system, contractors in all 50 states, insurance companies, and the IRS.

The FFM Service Desk, a multi-tier service desk, is managed and operated by Accenture in partnership with CMS. CMS is responsible for Tier 1 support. Accenture is responsible for Tier 2 and Tier 3 support using the Information Technology Infrastructure Library (ITIL) standards and framework. Additional support services include security, maintenance, and system interoperability. More than 50,000 issues were triaged and resolved by the FFM Service Desk between 2015 and 2022.

Accenture has successfully operated through seven open and special enrollment periods in collaboration with CMS and other FFM stakeholders to support 45 million+ enrollments and \$200 billion+ in total payments since 2015. Accenture's contract has been renewed three (3) times and is ongoing through January 10, 2026, and the contract value is \$1.36 billion over 12 years.

Reference Questions: For each question below, please provide a comment.

1. Did the Contractor produce high quality deliverables? Please describe briefly.

Accenture provides consistently high-quality deliverables. Accenture has received a quality score of "Exceptional" for seven consecutive years in the CMS CPAR system (Contract Performance Assessment Reporting system). Accenture has supported CMS through nine near-flawless open enrollment periods. Accenture's high quality is also instrumental in CMS' ability to support ongoing infrastructure, modernization, and policy needs. Recent infrastructure quality highlights include:

- Ongoing stable and high-quality operations to support eligibility determinations, enrollment, policy payment, and qualified health plan management.
- Accenture seamlessly conducted the transition-in activities for the new FFE contract without disrupting critical ongoing Marketplace operations and services.
- Accenture prioritized high-quality delivery in all aspects of their support for the Marketplace.
- Accenture has executed multiple architectural initiatives such as the new Encryption in Transit solution, advanced metric scaling capabilities to allow real-time infrastructure changes, critical software upgrades, and reduced the technical debt, all adding to the strength of the FFM/FFE system security, stability, and resiliency.

- Accenture recently successfully completed 13 upgrades across core FFM Systems to increase operational efficiencies and ensure the continuity of dependent business activities.
- Accenture ensured CMS' readiness to implement the new Multi-Factor Authentication in compliance with federal security mandates.
- Accenture enhanced the consumer eligibility & enrollment experience via modernized capabilities ahead of Open Enrollment 10, by providing App 3.0 solutions to resolve external UI errors.

2. Was the Contractor flexible and willing to work through issues during all stages of the Project?

Accenture has established a very comprehensive system monitoring to ensure the rapid identification and remediation of emerging issues. They flexibly respond to issues in collaboration with other key stakeholders to minimize disruption to ongoing priorities. CMS has recognized Accenture for 450+ notable achievements specifically related to their flexibility in supporting external vendors tackle unanticipated challenges.

Accenture has also demonstrated tremendous flexibility in various other aspects of delivery. Accenture is responsive to CMS feedback, and flexibly adjusts their team size and skills to best meet CMS' needs. Accenture quickly adapts to new CMS requirements and goes above and beyond to help other CMS contractors (not under contract with Accenture).

Accenture's flexibility helps maximize the success of the Federally Facilitated Marketplace. Overall, Accenture does an exceptional job of maintaining positive and productive working relationships at all levels with the CMS staff and management, as well as with the various other Marketplace Application Development Organization contracting teams.

3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.

Accenture's communication is excellent. Accenture has been recognized by CMS for 600+ notable achievements specifically related to communication. Accenture provides clear, timely and complete plans, status, and deliverables. Accenture appropriately identifies and escalates risks and provides CMS with clear mitigation approaches and impact assessments. Additionally, Accenture communicates key program information through a large number of weekly meetings that address all aspects of the program.

4. Were there any major issues with Key Staff turnover or replacement?

Accenture is excellent at managing program staff. They have a large number of highly qualified staff and always have the skilled staff CMS requires. Accenture manages any needed transitions smoothly. There have been no program performance issues related to personnel.

5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?

Accenture's team includes staff from ~20 subcontracting companies. Most of these companies are small businesses. Their involvement supports CMS' subcontracting objectives and contract-specific subcontracting goals. These subcontractors support all aspects of the program. Accenture has managed subcontractor personnel well, and they operate as a seamless team. There have been no program performance issues related to subcontractors.

6. Was the Project a success?

The FFM program is ongoing, and it continues to be successful. The program has adapted to recent policy requirements for the American Rescue Plan and the CARES act, while concurrently modernizing infrastructure and performing operations successfully.

7. Would you rehire/recommend this Contractor? If not, why not?

Yes, we would recommend Accenture.

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?

We would give Accenture a grade of 10. Accenture has received exceptional Contractor Performance Assessment Reporting System (CPARS) scores for Quality, Schedule, Management, and Cost Control for seven consecutive years.

Other Comments:

No additional comments.

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name	██████████
Title	████████████████████
Date	██████████
Signature	<div> <div>██████████</div> <div>██████████</div> </div>

FIRM REFERENCE: FIRM NAME	
Reference Agency Name: Federal Student Aid (FSA)	
Project Name: Title IV Origination and Disbursement (TIVOD)	
Contact Person/Title: [REDACTED] [REDACTED]	Phone: [REDACTED]
Address: [REDACTED]	Email: [REDACTED]

FIRM REFERENCE: FIRM NAME
Describe the services provided:
<p>Project Description</p> <p>Common Origination and Disbursement (COD) is the U.S. Department of Education's Office of Federal Student Aid's (FSA) suite of applications to determine eligibility for federal, post-secondary financial aid. Launched in 2003 as a mainframe-based solution, the system processes ~30 million award originations and ~60 million disbursements, totaling nearly \$145 billion in aid annually. To support this financial aid processing, COD includes three websites that provide online services to financial aid recipients and their families, staff at post-secondary institutions, and FSA employees. In 2015, these websites were accessed by over 12.5 million users.</p> <p>To enable cost savings, improve agility, and enhance the security posture, Accenture was hired as the Prime Contractor to modernize COD by re-architecting it to run on a fully automated, modern technology stack and host it on a FedRAMP authorized cloud service provider. The hosting transition occurred in 2015 to establish the DevSecOps platform vision of accommodating the change flexibility and pace expected by the contract. The resulting platform allowed a greater percentage of the available budget to be delivered directly to aid recipients, reducing administrative and operation costs for the federal aid programs, and more securely stored the information of its 83 million unique customers' PII.</p> <p>The realization of the updated platform provided the initial building blocks to enable the transition to AWS GovCloud in 2018. After the re-architecture, the platform evolved to include industry-leading technologies for execution, operations, and development architecture. These changes accommodated the pace of growth, expansion, and maintenance of over 40 applications. This effort included the establishment of a fully automated and containerized development architecture with a focus on DevOps enablement. The migration to AWS transitioned all core components within a single weekend.</p> <p>Since the successful transition, Accenture has assumed website hosting responsibilities from a client-contracted third-party vendor for StudentLoans.gov and ATS, the two public-facing websites which are used by 12.5 million unique users to complete transactions annually. Accenture also rebuilt ~50 school reports, ~400 client reports/queries, and internal operations reports and dashboards to utilize the new reporting data store. Accenture updated 27 interfaces with the new COD solution and converted ~18 billion records from legacy IMS/DB2 databases into a new Oracle- hosted data model with over 700 tables. The AWS system performance exceeds that of the legacy system across a wide variety of business functions and interface processing.</p>

Reference Questions: For each question below, please provide a comment.	
1. Did the Contractor produce high quality deliverables? Please describe briefly.	Yes, Accenture consistently provides high quality products and services. The work products and Deliverables that they submit are organized and in a clear and easy to read format. They ask and respond to questions regarding work products and Deliverables in a timely and consistent manner.
2. Was the Contractor flexible and willing to work through issues during all stages of the Project?	Yes, Accenture is consistently on or ahead of schedule for meeting milestones and delivering work products and Deliverables. They constantly work with FSA to set the schedules and are flexible when they need to be changed. When changes need to be implemented quickly, Accenture provides reasonable assessments and estimates for getting the work scheduled and completed.
3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.	Yes, Accenture provides proactive customer service to FSA and ensures that management of the project meets acceptable standards. They retain and promote staff to ensure all levels of workers and managers, and FSA staff are informed and involved in the process of delivering financial aid to FSA's customers.
4. Were there any major issues with Key Staff turnover or replacement?	No.
5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?	Yes, Accenture utilizes Small Businesses for both customer service and development work. Accenture is constantly looking for ways to improve services by using small businesses. Their customer service center solution provides an excellent avenue for maximum use of small business utilization.
6. Was the Project a success?	Yes, the overall move to the AWS platform as well as the day-to-day operations of the COD system has been a success.
7. Would you rehire/recommend this Contractor? If not, why not?	Yes, given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.
8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?	

Accenture's overall performance rating is: 10

Other Comments:

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name

[REDACTED]

Title

[REDACTED]

Date

[REDACTED]

Signature

[REDACTED] [REDACTED]

FIRM REFERENCE: FIRM NAME	
Reference Agency Name: Federal Student Aid (FSA)	
Project Name: Digital & Customer Care (DCC)	
Contact Person/Title: [REDACTED]	Phone: [REDACTED]
Address: [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project Objective</p> <p>The U.S. Department of Education (ED) is the agency responsible for education policy within the U.S. Federal Government. ED establishes federal education funding policies, administers and monitors funds, oversees research on America's schools, and focuses national attention on important issues in the American education system.</p> <p>One of ED's key roles in postsecondary education is to determine eligibility for Title IV federal student aid for eligible students and their families. The Office of Federal Student Aid (FSA) is the organization within ED that is responsible for managing Title IV. FSA originates over \$115 billion federal grants, loans, and work-study funds to approximately 10.8 million students at more than 5,600 participating postsecondary schools annually.</p> <p>Historically, federal student aid has been challenging for borrowers to navigate. There were multiple websites with different information that lacked a consistent look, feel, and approach to engage or assist customers. To tackle this, ED created a Next Generation Financial Services Environment (Next Gen) in 2018 – an innovative, streamlined, world-class solution to benefit customers, parents, financial aid administrators (FAAs), and other school partners that work with FSA. The goals of this transformation include achieving greater operational and technical flexibility, cost efficiencies, a consistent and intuitive customer experience, and better outcomes for all stakeholders.</p> <p>Accenture is working with FSA to carry out this critical overhaul of all digital and customer care (DCC) touchpoints. Accenture is working with FSA to create a single phone number for unified point of access and a modernized customer care platform (CCP). On average, this streamlined capability transfers over 3.5 million inbound calls annually, allowing customers and their families to reach a variety of call centers supporting different lines of business. In addition, Accenture is working with FSA to create a single digital front door that consolidates the FSA loan and grant processes. To date, FSA and Accenture have consolidated processes available across FAFSA.ed.gov, FSAID.ed.gov, StudentAid.gov, StudentLoans.gov, BorrowerDischarge.ed.gov, and the NSLDS.ed.gov websites into a single website. In addition, Accenture and FSA have collaborated to create "Aidan," a conversational artificially intelligent (AI) virtual assistant (VA). This is the first use of a VA in the federal loan process by the government, enabling self-service without human intervention. Finally, an updated Marketing and Communications Platform (MCP) delivers personalized communications across a variety of channels including email, short message service (SMS), and social. The MCP sends over 290 million emails annually to customers with a 2021 peak of 5.5 million in a single day.</p>	

Reference Questions: For each question below, please provide a comment.	
1. Did the Contractor produce high quality deliverables? Please describe briefly.	<p>Yes, the accomplishments and deliverables as part of this contract were significant, with releases on an average of every two months that included major customer improvements such as the Loan Simulator and Annual Student Loan Acknowledgement. The mobile app and StudentAid.gov were enhanced, allowing FSA to retire legacy websites. A new employer database was added to the Public Service Loan Forgiveness Help Tool, allowing borrowers to know understand their eligibility for the program prior to applying. The Virtual Assistant was made available to more users enabling self-service and the customer care platform onboarded additional contact centers. All of this was done during a global pandemic. Overall, Accenture successfully delivers on the scope of the contract, including quality deliverables and work products that meet the needs of Federal Student Aids more than 40 million students, parents, and borrowers.</p>
2. Was the Contractor flexible and willing to work through issues during all stages of the Project?	<p>Yes, Accenture has been able to meet the schedule agreed to with Federal Student Aid, including multiple releases with overlapping schedules for which they stayed on track. In one case, the government significantly changed requirements very close to a release date. Accenture was flexible in accommodating the new requirements and was able to expedite the schedule to meet expectations. The result was an improved experience for borrowers to apply for one of FSAs loan forgiveness programs. Additionally, Accenture worked with FSA to respond quickly during the pandemic by getting out communications to FSA customers across multiple customer channels. As a result, over 270 million emails were sent in FY20 to ensure borrowers were aware of the loan payment pause and 0% interest rate under the CARES Act.</p>
3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.	<p>Accenture management is customer service- oriented, communicative, and responsive. Program management and risk management practices are coordinated and thorough. Requests for changes have been met with flexibility. Any actions requested by FSA have been executed in a cooperative and expedited manner based upon business needs.</p>
4. Were there any major issues with Key Staff turnover or replacement?	<p>No, key personnel meet the qualifications needed and are effective in their roles. Accenture management closely interacts with Federal Student Aid to work out any issues raised with key staff turnover or replacement.</p>
5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?	

Although this contract does not have a small business subcontracting plan, Accenture diligently works to support small businesses as documented in their requests to subcontract.

6. Was the Project a success?

Yes, this project was a success. The first year of the contract established the foundational platforms and capabilities that enabled success in the second year. The foundation included a single 1-800 number through which customers can reach any FSA contact center, a consolidated digital platform on StudentAid.gov, a command center that provides visibility into contact center data, a customer relationship management tool that provides a 360-degree view of customer interactions, and a marketing and communications tool that provides streamlined and personalized email and text message communications. Outcomes include operational stability, rapid delivery at scale, and continuous innovation.

The second year of the contract included six releases, an average of one release every two months. New features were launched including the Loan Simulator and the Annual Student Loan Acknowledgement. The myStudentAid mobile app was enhanced and its functionality expanded beyond the FAFSA. Legacy websites such as Feedback.ed.gov and BorrowerDischarge.ed.gov were retired as the content and functionality were consolidated into StudentAid.gov. A new employer database was added to the Public Service Loan Forgiveness Help Tool. The Virtual Assistant was made available to more users and the customer care platform onboarded additional contact centers.

The flexibility of the platforms allowed FSA to respond quickly when the pandemic hit and the CARES Act was passed, which included payment suspension and 0% interest for over 40 million of FSAs customers starting in March 2020. Communications were shared across multiple customer channels, including web, email, text, postal mail, social media, and paid media. Over 270 million emails were able to be sent in FY20 and FSAs new Virtual Assistant was able to answer thousands of questions about COVID-19 impacts.

7. Would you rehire/recommend this Contractor? If not, why not?

Yes, I can attest to the great customer service provided in the areas of project management, contract administration, cost, and delivery under compressed timeframes.

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?

10

Other Comments:

REFERENCE AFFIRMATION AND SIGNATURES	
The undersigned hereby certifies that the foregoing statements are true and correct.	
Print Name	[REDACTED]
Title	[REDACTED]
Date	[REDACTED]
Signature	[REDACTED]

FIRM REFERENCE: ACCENTURE	
Reference Agency Name: State of California Consortium IV (C-IV)	
Project Name: Statewide Automated Welfare System (SAWS) C-IV	
Contact Person/Title: [REDACTED]	Phone: [REDACTED]
Address: [REDACTED] [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project description</p> <p>In 2001, the Statewide Automated Welfare System (SAWS) Consortium-IV (C-IV) began a project to design and implement a web-based integrated eligibility system to administer a variety of programs in California, including cash assistance (CalWORKs/TANF), food assistance (CalFresh/SNAP), medical assistance (Medi-Cal/Medicaid), and other state and county-specific programs.</p> <p>The C-IV system was implemented in all four original counties by October 2004. Subsequently, the ISAWS Migration Project (which included the 35 former ISAWS counties) began in September 2007 and concluded in August 2010. The C-IV system was shut-down as of September 2021, with the migration of the 39 counties to the CalSAWS platform.</p> <p>Technical solution</p> <p>The C-IV System integrated custom Java code with multiple COTS applications (e.g., Oracle database and middleware products, Adobe LiveCycle, Perceptive ImageNow, AWS Connect, and IBM Operational Decision Manager). Additionally, the core eligibility application interfaced with other custom applications (e.g., OCAT, Child Care Portal, and C4Yourself). The system had more than 50 batch and real-time interfaces with external systems including the Statewide Client Index, EBT Host-to-Host, and CalHEERS. At its peak, C-IV supported over 10 million transactions daily. The C-IV system included a multi-tiered processing architecture, a presentation tier optimized for multiple user interface platforms (web browsers, tablets, kiosks), an application tier, and a data tier.</p> <p>As of year-end 2021 (end of contract), this system was used by 39 California counties and served approximately 30% of California's public assistance caseload (approximately 4.8 million Californians). The C-IV System supported over 18,000 internal system users across more than 250 public assistance offices. The C-IV contract value for its 20-year period was over \$1.87 billion.</p> <p>Accenture services delivered</p> <p>Accenture was contracted in 2001 to work on all Design, Development, and Implementation (DDI) activities. Accenture completed implementation of the C-IV system in all four original counties by October 2004. Merced County became operational in March 2004; Stanislaus County in April 2004; Riverside County in August 2004; and San Bernardino County in September 2004. Following the successful implementation of the system, Accenture continued to perform</p>	

FIRM REFERENCE: ACCENTURE

application maintenance and maintenance and operations (M&O) services. After the ISAWS counties selected C-IV as their future system, the ISAWS Migration Project began in September 2007 and concluded on schedule in August 2010, with 39 counties successfully using the C-IV System.

As prime contractor for systems integration and M&O, Accenture was responsible for system modifications, system engineering, capacity planning, performance testing and monitoring, batch processing, security, hardware and software management, project management, and a service desk (tiers 1, 2 and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework.

During the contract, Accenture collaborated with multiple contractors responsible for different areas of the system such as Solutions West for training, Hyland Software for maintenance and support for their Perceptive Content solution, Gainwell for central print services, and First Data for QA services. Accenture's responsibilities included the core C-IV eligibility system, C4Yourself—the online portal for applications, an integrated contact center, and imaging technologies, as well as key integrations with the OCAT, CalHEERS, EBT systems, and kiosks and tablets in county lobby areas.

Reference Questions: For each question below, please provide a comment.

1. Did the Contractor produce high-quality deliverables? Please describe briefly.

Yes, Accenture has produced high quality contract and project deliverables, meeting expectations. Ongoing application releases were very high quality.

2. Was the Contractor flexible and willing to work through issues during all stages of the Project?

Yes. Accenture was a reliable partner to the C-IV counties.

3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.

Yes. Accenture communicated in a professional manner, and was timely, complete, and effective.

4. Were there any major issues with Key Staff turnover or replacement?

Accenture retained a robust pool of talent to successfully deliver and maintain the C-IV system.

5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?

Yes. Accenture leveraged a key subcontractor to provide Help Desk, central print, and remote maintenance support. No mediation was needed.

6. Was the Project a success?

Yes, Accenture successfully met its requirements, and consistently met service level agreements.

7. Would you rehire/recommend this Contractor? If not, why not?

Yes.

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?




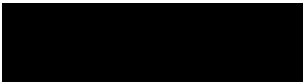
9

Other Comments:

--

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name	
Title	
Date	
Signature	

FIRM REFERENCE: STATE OF ARIZONA, ARIZONA HEALTH CARE COST CONTAINMENT SYSTEM (AHCCCS)

FIRM REFERENCE: FIRM NAME

Reference Agency Name:

State of Arizona: Arizona Health Care Cost Containment System (AHCCCS)

Project Name:

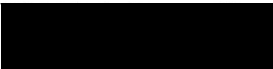

HEAplus M&O

Contact Person/Title:

[REDACTED]

Phone:

[REDACTED]

Address: 	Email: 
<p>Describe the services provided:</p> <p>Health-e-Arizona Plus (HEAplus) is the State of Arizona's eligibility determination and case management system that administers public assistance benefits for the Arizona Health Care Cost Containment System (AHCCCS) and the Arizona Department of Economic Security (ADES) agency. HEAplus provides a web-based portal for consumers, eligibility workers, and community assistors and supports eligibility determinations and ongoing case management for benefit programs, including Medicaid, Children's Health Insurance Program (CHIP) (known as KidsCare in Arizona), Medicare Savings Program (MSP), Arizona Long-Term Care System (ALTCS), MyFamilyBenefits (Electronic Benefits Transfer [EBT] portal), SNAP, and TANF.</p> <p>HEAplus collaborates with county departments and non-county medical assistance (MA) sites to administer MA programs throughout the State of Arizona, as well as the SNAP and TANF programs. The objective of the project is to offer the most accurate, credible, real-time eligibility determinations for the State, which serves over 3,900 internal state workers and over 2.43 million Arizonans, 1.75 million of whom use the portal (including multiple user groups from the worker portal and self-service portal). The system processes 22,250 daily eligibility cases. AHCCCS is a \$20 billion program.</p> <p>In October 2020, the AHCCCS, the Medicaid agency responsible for HEAplus, awarded Accenture an initial five-year M&O (Maintenance & Operations) contract to maintain the system by bringing transparency and efficiency to the overall operations of the system. The contract includes the end-to-end maintenance, operations, and enhancements of all system components. Accenture, the Prime Contractor, worked with the incumbent to transition the support of the IaaS footprint for the State of Arizona to Microsoft Azure Cloud. After the successful transition, Accenture began providing comprehensive services to maintain the HEAplus system in Azure Cloud with greater scalability and flexibility for business and policy initiatives. The contract supports a multi-vendor design (AHCCCS, DES & Department of Correction).</p>	
<p>Reference Questions: For each question below, please provide a comment.</p> <p>1. Did the Contractor produce high quality deliverables? Please describe briefly.</p> <p>All deliverables were provided as expected and met the acceptance criteria. As a result, the deliverables would be considered high quality. There were several instances where the contractor provided additional deliverables or information above what was requested in the RFP.</p>	
<p>2. Was the Contractor flexible and willing to work through issues during all stages of the Project?</p>	

There were many twists and turns during the transition from the outgoing vendor outside of Accenture's control and they willingly adapted to course corrections.

3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.

There were several communication standards defined in the RFP (status updates written, status update meetings, communication plans, etc.) The contractor met all the communication requirements timely and also provided adhoc updates and suggestions throughout the project. In summary, the communication was timely, complete and effective.

4. Were there any major issues with Key Staff turnover or replacement?

No

5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?

All key personnel were contractor employees not sub-contractors. All the Contractor staff that the state personnel worked with directly were contractor employees. Subcontractors were used on the project but not in key positions. It was limited to a few technical positions and those resources appeared to be managed effectively.

6. Was the Project a success?

The project was successful. It met all the required deliverables with less than anticipated disruption. The transition was completed approximately a month earlier than scheduled.

7. Would you rehire/recommend this Contractor? If not, why not?

We are not permitted to supply opinions or speculation when completing contractor evaluations. That being said, the contractor is in good standing with the State and is eligible for additional services/contracts.

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?

We are not permitted to supply opinions or speculation when completing contractor evaluations. We do not have an official mechanism to rank contractors on this scale. The contractor met all their contractual duties, and the project was completed ahead of schedule and on budget. All deliverables were accepted/approved by the State.

Other Comments:

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name

Title

Date

Signature

FIRM REFERENCE: ACCENTURE	
Reference Agency Name: California Statewide Automated Welfare System (CalSAWS) Consortium	
Project Name: California Statewide Automated Welfare System (CalSAWS) (prior project name was the LEADER Replacement System (LRS), which is now called CalSAWS)	
Contact Person/Title: [REDACTED]	Phone: [REDACTED]
Address: [REDACTED] [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project description</p> <p>The California Statewide Automated Welfare System (CalSAWS) is an integrated eligibility system built and operated by the CalSAWS Consortium on behalf of the 58 counties of California. CalSAWS supports the counties in administering public assistance programs in California, including cash assistance (CalWORKs/TANF), food assistance (CalFresh/SNAP), medical assistance (Medi-Cal/Medicaid), and other state and county-specific programs.</p> <p>The system first went live in 2015 in Los Angeles County, and at that time, it was known as the LEADER Replacement System (LRS). Migration from an on-premises data center to cloud hosting occurred on October 14th, 2019.</p> <p>Technical solution</p> <p>CalSAWS is the most extensive integrated eligibility system in the United States and is hosted in the Amazon Web Services (AWS) cloud. The CalSAWS core eligibility application includes a multi-tiered processing architecture, a presentation tier optimized for multiple user interface platforms (e.g., Google Chrome and Microsoft Edge), an application tier, and a data tier. Other components of the system run on other user interface platforms such as kiosks and tablets. The system integrates custom Java code with multiple COTS applications (e.g., Oracle database and middleware products, Informatica Identity Resolution, Pitney Bowes Spectrum, ForgeRock, Adobe Experience Manager, AWS Connect, and IBM Operational</p>	
FIRM REFERENCE: ACCENTURE	
<p>Decision Manager). The core eligibility application further integrates with other custom applications (e.g., The core eligibility application further interfaces with other custom applications (e.g., OCAT, Child Care Portal, and BenefitsCal).</p> <p>Supporting over 10 million transactions daily, CalSAWS has more than 50 interfaces, six of which are real-time. The system is currently in production in 42 counties. The system is used by 18,500 internal users daily across 125 locations to support 11 million Californians who receive public assistance. CalSAWS issues more than \$1 billion in benefits each month.</p> <p>By October 2023, all 58 counties will have migrated to this platform. After all counties are migrated to CalSAWS, 41,000 internal users will use CalSAWS daily to support approximately 19 million Californians and issue approximately \$2 billion in benefits each month.</p>	

Accenture services delivered

Accenture is one of seven contractors responsible for CalSAWS and has the largest scope of work. Accenture's contract began in November 2012 and is ongoing through April 2025. The contract value is approximately \$1.425 billion. As the prime contractor for systems integration and maintenance and operations (M&O), Accenture is responsible for application maintenance and system enhancements, and cloud-based operations including network engineering, cybersecurity vulnerability mitigations, capacity planning, performance testing and monitoring, and batch processing. Accenture supports hardware and software management, system engineering, data conversion, and project management. Accenture also supports the service desk (tiers 1, 2 and 3) using the Information Technology Infrastructure Library (ITIL) standards and framework.

Accenture is responsible for the core CalSAWS eligibility system, the analytics application, ForgeRock identity solution, contact center technologies, Child Care Portal, and kiosks/tablets in several county lobbies. The CalSAWS Consortium has separate prime contracts for legacy system maintenance (CalWIN), cloud hosting, the public portal (BenefitsCal), imaging (SaaS contract), OCAT, GA/GR Correspondence solution, and print services.

Reference Questions: For each question below, please provide a comment.

1. Did the Contractor produce high quality deliverables? Please describe briefly.

Yes, Accenture has produced high quality project deliverables, meeting expectations.

2. Was the Contractor flexible and willing to work through issues during all stages of the Project?

Accenture has been a reliable partner to the CalSAWS Consortium and our member counties. They acknowledge and work through system performance issues as quickly as possible. However, when updates to requirements were applied, the team did not follow the scope management process timely.

3. Was communication between the Contractor and your organization's Staff open, timely, complete, and effective? Please briefly summarize.

Accenture staff communicate in a professional manner and can effectively convey technical solutions to business partners and stakeholders. However, advance notice of database sizing issues and corresponding cost impacts were not brought forward timely.

4. Were there any major issues with Key Staff turnover or replacement?

Accenture has retained strong Key Staff talent at the Director level. However, limitations with certain knowledge areas have led to inefficiencies with management of the Consortium's AWS accounts with cost impacts, hardware & software inventory tracking, production operations, and process/control documentation gaps.

Reference Questions: For each question below, please provide a comment.	
5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?	
Yes. Accenture has leveraged a key subcontractor to provide Help Desk and remote maintenance support. Additional subcontractors are used in the areas of imaging and staff augmentation. No mediation has been needed.	
6. Was the Project a success?	
Yes. Accenture successfully moved the LRS to a cloud-based platform and migrated the former C-IV counties to CalSAWS, as well as two of the CalWIN counties to date. The application release quality is very high.	
7. Would you rehire/recommend this Contractor? If not, why not?	
Yes.	
8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?	
8	
Other Comments:	
REFERENCE AFFIRMATION AND SIGNATURES	
The undersigned hereby certifies that the foregoing statements are true and correct.	
Print Name	
Title	
Date	
Signature	

FIRM REFERENCE: ACCENTURE	
Reference Agency Name: State of Kansas, Department of Health and Environment (DHE)	
Project Name: Kansas Eligibility Enforcement System (KEES)	
Contact Person/Title: [REDACTED]	Phone: [REDACTED]
Address: [REDACTED] [REDACTED]	Email: [REDACTED]
<p>Describe the services provided:</p> <p>Project description</p> <p>The Kansas Eligibility Enforcement System (KEES) is a health and human service eligibility system that was developed and implemented to administer the full suite of human service programs. The system first went live in a phased approach, with its first go-live in July 2012 and the final go-live in August 2013. This includes Food Assistance (SNAP), Temporary Assistance for Needy Families (TANF), Child Care, Employment Services, Food Assistance, Employment and Training (FAET and GOALS), Low Income Energy Assistance Program (LIEAP), Automated IV-E Eligibility, Medical assistance programs, including Medicaid (MAGI, E&D, and LTC), CHIP, KanCare, AIDS Drug Assistance Program (ADAP), and several other state-funded programs.</p> <p>The Kansas Department of Health and Environment's (DHE) Division of Health Care Finance and the Kansas Department for Children and Families (DCF) administers human service and medical assistance (MA) programs that serve over 720,000 Kansans annually. In the last two years, the KEES has distributed over \$814 million in benefits to Kansans.</p> <p>The KEES system provides Kansans with greater integration across its programs and online access to health information as an alternative to office visits. The system generates savings through more efficient eligibility processing and much-improved decision-making and compliance controls. Through a flexible and modular technology approach, KEES helps the state more readily and cost-effectively update the eligibility system as Kansan's needs and government policies change over time.</p> <p>Technical solution</p> <p>In January 2020, Accenture migrated KEES onto Oracle Cloud after a nine-month design and implementation process. Within Oracle Cloud, Platform as a Service (PaaS) and Software as a Service (SaaS) are used for application delivery. The Core Logging as a Service (LaaS) solutions aggregate components run on Linux and Microsoft Windows. The large and complex solution integrates custom code with multiple COTS applications (e.g., Adobe Experience Manager, Oracle Intelligent Advisor, Oracle Address Verification, Oracle Analytics, Stone Branch, etc.), including the citizen-facing portal, worker eligibility system, and COTS eligibility software.</p> <p>This platform has several portals supported by multi-tiered processing, including a user-facing application optimized for multiple user interface platforms (e.g., laptops and mobile devices). The platform interfaces with over 25 major external systems, including state and local partners for income information, federal partners for social security data, the KMMS (MMIS) system for</p>	

Kansas, and the federal hub (which is **real-time**). There are **2,500 internal** and **tens of thousands of external users** in **multiple locations**.

Accenture's services delivered

Accenture's contract began in September 2011 and is ongoing through August 31, 2024, with a contract value over **\$100 million**. As the **prime contractor** for KEEs, Accenture performs application maintenance, system modifications, cloud-based operations, cybersecurity vulnerability mitigation, network and system engineering, capacity planning, performance testing, performance monitoring, and batch processing. Accenture is also responsible for application design, development, testing, change management, training, conversion, and running a **service desk (tiers 1, 2, and 3 via ServiceNow)** using the Information Technology Infrastructure Library (ITIL) standards and framework. Accenture continues to serve as the prime maintenance and operations vendor responsible for ongoing system maintenance, security, deployments, and enhancements providing day-to-day system operations through effective project management, governance, and communication with Kansas DHE. Accenture has implemented innovative solutions outside of their original scope, such as digital imaging and artificial intelligence (AI) bots. Accenture is overseeing a project at Kansas DCF to develop an Amazon Chime chat and an enhanced virtual contact center to provide Kansans with an enhanced customer service experience, and to enable agents to handle increased call volume from anywhere.

Reference Questions: For each question below, please provide a comment.

1. Did the Contractor produce high quality deliverables? Please describe briefly.

Deliverables fall within accepted guidelines and meet requirements. Accenture has also been willing to listen and adjust processes if there are suggestions for quality improvements or better efficiency in an area.

2. Was the Contractor flexible and willing to work through issues during all stages of the Project?

Accenture is very flexible and has shown throughout their engagement a willingness to adjust priorities, processes, and resources to fit the needs of the work and the overall team. They are highly engaged with issues and show a quick response as well as a high level of solutioning ability.

3. Was communication between the Contractor and your organization's Staff open, timely, complete and effective? Please briefly summarize.

Accenture communicates appropriately based on the situation and provides all relevant information. They are very open to feedback and willing to adjust if we have a different request. They are also highly responsive to questions and other requests. Overall, Accenture does an effective job communicating. Their presentations are informative, and they adapt to different audiences.

4. Were there any major issues with Key Staff turnover or replacement?

No issues related to turnover. Key staff turnover is low. In the event where turnover did occur, Accenture had a skilled replacement to transition to.

5. Were any Subcontractors used by this Contractor? If so, for what purpose/major tasks? How well did the Contractor manage its Subcontractors and did your organization ever have to mediate?

Subcontractors are used, mainly for technical components. Since our transition to Oracle Cloud Infrastructure in 2020, Oracle is the largest subcontractor for Accenture on our account. The subcontractors are seamless to us, as Accenture manages them effectively and no state intervention is required.

6. Was the Project a success?

The initial project was delivered in three main phases. Since that time, we have continued to complete enhancement work, transitioned to a cloud hosting environment, and completed a major upgrade. All of these activities were considered to be successful.

7. Would you rehire/recommend this Contractor? If not, why not?

Yes, we would hire Accenture again. This vendor has met all of their contractual obligations, and they have shown a dedication to quality improvement and a willingness to be flexible and adapt to changing circumstances

8. On a scale of 1-10, with 1 being the lowest and 10 being the highest, how would you rate this Contractor's overall performance?

I would score this contractor as an 8. Accenture meets their contractual obligations consistently. They have been a very attentive and flexible partner to work with. If an issue does arise, they are responsive and take action to correct it. There are also examples where they have gone beyond the service expected to provide more robust solutions, as in the case of system monitoring for performance. They have also demonstrated a lot of flexibility with planned enhancement releases, as priorities can change quickly as new regulations and policies occur.

Other Comments:

--

REFERENCE AFFIRMATION AND SIGNATURES

The undersigned hereby certifies that the foregoing statements are true and correct.

Print Name	
Title	
Date	
Signature	