**RFP 20-1351**

**TECHNICAL PROPOSAL**

**ATTACHMENT F**

**Instructions: Please supply all requested information in the areas shaded yellow and indicate any attachments that have been included to support your responses.**

* + 1. **General Requirements and Definitions**
       1. Please confirm your understanding and acceptance to all definitions and abbreviations listed in RFP Section 1.2. Please list any additional terms and definitions used by your company or industry that you would like the State to consider incorporating in the contract. The State will not accept terms and definitions introduced after award during contract finalization and implementation.

|  |
| --- |
| NIC Indiana confirms that we have read, understand, and accept all definitions and abbreviations listed in RFP Section 1.2. |

* + - 1. Please confirm you have carefully reviewed all requirements listed in RFP Section 1.4, Attachment J- Scope of Work and Attachment J1- Scope of Work-Security. Should your company have any exceptions, substitutions, or conditions for the State’s consideration, please list them below. The State will not accept exceptions, substitutions, or conditions introduced after award, during contract finalization and implementation.

|  |
| --- |
| NIC Indiana has carefully reviewed all requirements listed in RFP Section 1.4, Attachment J- Scope of Work and Attachment J1- Scope of Work-Security and does not have any exceptions, substitutions, or conditions for the State’s consideration. |

* + - 1. Please confirm your understanding of the secondary competitive process as outlined in Attachment J- Scope of Work, Section 1.4.3 (Secondary Competitive Process). Please provide examples of mitigation strategies your company has implemented to help customers offset the operational and budget challenges associated with transitioning and integrating with a new payment processor. Please provide an example of an individual implementation plan and timeline your company has utilized in the successful transition of customers.

|  |
| --- |
| NIC Indiana has read and understands the secondary competitive process defined in Attachment J.  Example Mitigation Strategies  Examples of mitigation strategies to help offset the operational and budget challenges associated with transitioning and integrating with a new payment processor include:   * The NIC Payment Platform is designed to be integrated into existing government services; a suite built on the needs of our government partners. Using decades of experience in the public sector, NIC will work to analyze all existing systems and select an integration approach and/or product that best fits each agency’s unique needs. * Based on experience with other statewide payment implementations, NIC Indiana is proposing a phased approach based on the unique requirements of each payment engagement, with a focus on ensuring dependencies are addressed early on to ensure a streamlined transition as services are onboarded. * NIC Indiana has an experienced local team dedicated to the successful transition and integration of the State of Indiana’s services to the NIC Payment Platform. NIC resources will be readily available to consult with each agency, test online products, and validate installation of point-of-sale devices in the field to ensure the needs of each agency are met. * The local team has extensive experience with integrating the NIC Payment Platform with existing state or third-party systems. The suite of payment processing products has been leveraged by NIC’s government partners across the country and are designed for efficient and streamlined integration using standards-based technologies. * NIC Indiana provides low risk, proven implementation services to participating agencies that minimize the need for agency resources and follow robust processes that have been effective in Indiana and across the country. These services will provide management and guidance for on-boarding to the NIC Payment Platform, data transfers, batch files, training, reporting, compliance with PCI DSS requirements and more. * As with any project, NIC Indiana will work with each participating agency on an individual basis to establish and identify any risks to the implementation and transition. * As a general best practice, NIC believes that the State should assign a Program Manager to oversee all activities and meetings. This has proven a successful strategy in other implementations. For example, in Florida, the State Treasurer (contract agency) assigned a Program Manager who schedules all meetings with the agencies and has been critical to the project’s success through agency participation and timeliness. NIC Indiana can assist the state with these duties through the use of our local resources, including our MBE/WBE/IVOSB partnerships as needed.   Example Implementation Plan & Timeline  When new agencies or expansion of services are on the horizon, NIC Indiana will scale our proven implementation approach to ensure that the new NIC Indiana service or expansion is deployed on time, with high quality, within the mutually agreed upon implementation timeframe.  Our detailed implementation plan for new services as a program expansion or new program within a state agency is similar to the implementation plan for migration of services. In many instances, implementation activities may be streamlined or may no longer be required. For example, using a current merchant account, a current bank account and disbursement set-up, and current POS devices will significantly streamline the implementation duration. NIC Indiana can also use Soft Descriptors, which allows an agency to use an existing merchant account and create a new service description to display on the customer statement thus eliminating the need and time required to provision a new merchant account. Training may be reduced if the agency users are using the NIC Payment Platform for other existing services.  The below checklist represents the key aspects of implementation of service or program expansion within a state agency.  Implementation Checklist   * Kickoff Meeting with Stakeholders * Discuss overall objectives * Confirm Merchant of Record Services * Confirm Flow of Funds * Discuss application integration methods * Prioritize services * Identify all settlement and post-capture data * If applicable, board new merchant accounts * If applicable, begin Financial Disbursement Testing * If applicable, establish bank disbursement profile accounts * Set up Merchant/Services in TEST/PROD TPE * Integration to NIC Payment Platform * Provide Integration API/Guide and support to State to develop integration * Test Integrations and POS Devices * Stage application in production environment * If applicable, conduct end-to-end testing of live transactions * Discuss and Schedule Training or Training Refresher * Develop State Entity specific training plan * Administer testing plan for financial admin/reconciliation * Conduct State Entity training * Deployment Activities * Project Close Documentation * Production Support Processes   Example Implementation Plan & Timeline  Following is an example implementation plan and timeline utilized in one of NIC’s other payment processing implementations: |

* + 1. **Service Overview and General Scope**
       1. Please describe your company's experience with state government fee structure-based credit card processing, specifically through web, IVR, and POS transactions.

|  |
| --- |
| NIC has operated the multi-channel NIC Payment Platform technology proposed for Indiana under government fee-structure based credit card processing for 20 years. The NIC Payment Platform is a PCI DSS compliant Software-as-a-Service (SaaS) solution and NIC Services is a PCI DSS Level 1 Service Provider. Over the years, we have continually improved the solution based on changes in payment channels and technology, security, user expectations, and government needs. The result is a modular architecture that can rapidly implement new technologies, and a comprehensive operations and security approach that leverages experienced staff, third-party experts, tools, and processes to stay ahead of the ever-changing world of government e-commerce.  These government payment services encompass a wide variety of payment channels including web, mobile, IVR, and POS installations, and most of our implementations include all of these payment channels. Additionally, NIC continues to develop solutions to meet the unique needs of our government partners such as offline capable mobile payment processing for rural payments without access to Wi-Fi or cellular service, SMS initiated payments, eWallet, and more.  NIC Indiana intimately understands payment processing in a government environment and supports Convenience Fee, Merchant Model and Flat Rate payment options which can very down to each individual service. This has been proven in Indiana and for each of the thousands of government agencies we support. Each of our government partners determines the payment flow of funds and fee structure that best fits their service’s needs and the type of service they are providing. This includes determining what payment types to turn on for each service and setting up a service with the specific convenience fee or merchant model. NIC is the largest purely government payment provider in the U.S. and works closely with our processors and the card networks to provide the best options given the specific nuances and rules for each payment type.  As the preferred payment platform provider for more than half the states in the U.S. — more than 176 million Americans, 54% of the total U.S. population — NIC has led the transformation to frictionless delivery digital government services and is the largest payment processor solely focused on government, and, in 2020 alone, we securely processed more than 402 million transactions worth $24 billion. All told, NIC provides comprehensive payment processing services at the state and local level in 32 states, as well as payment services for projects on behalf of 15 federal agencies including Recreation.gov. |

* + - 1. The Contractor must provide its own Payment Processing Solution. The State prefers applications on the PCI Validated Payment Applications list (<https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true> ). Please provide a detailed description of your payment processing solution.

|  |
| --- |
| A Proven PCI DSS Compliant Payment Application  The NIC Payment Platform provides a centralized NIC TPE® Payment Engine gateway, administration, settlement, disbursement, and reporting module.  The NIC Payment Platform includes the following modules:   * Over-the-Counter (OTC) module for Point of Sale transactions * Common Checkout Pages (CCP) module for customized online web payment pages * Customer Database (CDB) module for billing and recurring payments * Prompt Pay module for SMS and email-based payments for citizens * OnTheGo® Pay module for taking POS credit and debit card payments on a mobile device in the field * Gov2Go® Pay digital wallet that streamlines government payments * Fiserv CheckFreePay integration offers the ability to accept cash through Fiserv’s CheckFreePay agent network   Description  The NIC Payment Platform is a fully hosted, software-as-a-service, enterprise-class payment processing solution that provides merchant processing, payment gateway, and many other e-commerce features, all specifically designed to meet the needs of digital government programs. The NIC Payment Platform is annually certified by a third-party PCI Qualified Security Assessor to the Payment Card Industry Data Security Standards (PCI DSS) as a Level 1 Service Provider. NIC is listed as a PCI DSS Compliant provider on Visa and MasterCard's Global Registry of Service Providers, and leverages a third-party to perform a SOC 2, Type 2 assessment across the NIC payment processing environment. Additionally, NIC only uses PCI DSS compliant payment processors to process payment transactions.  The NIC Payment Platform has comprehensive reporting tools that support operational and financial agency needs. Designed to automate and streamline the bank reconciliation processes, this solution reduces the amount of time it takes to complete reconciliation and provides financial transaction transparency. The NIC Payment Platform central repository of transactions allows the agency to integrate efficiently with backend processes, as well as to adhere to industry‐standard accounting and audit processes. Within this module, all payment processing data is made available via a wide variety of reporting features. Reports range from summary reports to detail reports showing line item level data.  The NIC Payment Platform provides the payment capability for thousands of digital government services across the U.S. and is the foundation of the financial processing capabilities of Indiana online services across the State whenever payment collection is needed. Credit cards, debit cards, and e-checks are all supported with the flexibility to integrate other emerging payment methods as needed. The NIC Payment Platform provides flexible integration options including shared Common Checkout Pages (CCP), which shield applications from exposure to payment information, the DirectConnect API for non-web applications, and special integration methods for point-of-sale devices. The NIC Payment Platform connects to a financial processor’s services to perform the backend presentment of transactions to the networks. The NIC Payment Platform is more than just a payment processing gateway, though. It is a full featured service for managing and accounting for the full lifecycle of payments, designed specifically around the special needs of government entities.  PCI DSS Assessment Validation  NIC Services owns and operates the payment processing platform providing processing services to NIC Business units and Partners. The platform is certified as a PCI Level 1 provider driven largely by the high quantity of transactions the NIC payment platform manages per card brand per year. The platform and components that support all processing functions are architected, managed, and maintained by NIC and are utilized as part of the Payment Processing services that NIC provides. Because processing with NIC is a service-based engagement, each individual component or application is not classified as Payment Applications under the PCI PA-DSS validation program. Rather, the components and applications are included in an annual PCI DSS assessment that NIC has performed on the environment as required by the Card Brands. This assessment is performed by a PCI Qualified Security Assessor (QSA) and a Report on Compliance (ROC) is issued and submitted to the Card Brands annually. The ROC has an Attestation of Compliance (AOC) section that is utilized to demonstrate compliance to customers and partners and NIC Services is also listed as a Validated Service Provider on both Visa and MasterCard’s websites.  NIC Indiana understands the PA-DSS program is ending and is being replaced by the Secure Software Standard. In the event the NIC Payment Platform is a candidate under the Secure Software Standard, NIC will comply with any applicable standards under that program when it is implemented. |

* + - 1. Please provide details on your ability to integrate with the State standard middleware products including, MuleSoft and other comparable products, to provide (or develop) an API solution for State connectivity. Include details on your experience with MuleSoft, or comparable middleware products.

|  |
| --- |
| The NIC Payment Platform offers flexible and configurable integration methods to ensure maximum utility, provides the necessary gateway and connections to merchant processing services to fuel the transactions, and the enhanced visibility through reports and reconciliation tools to allow agency payment experts to manage the entire lifecycle of payments. The proposed platform offers modules built specifically for government to support over the counter, online, kiosk, mobile, subscription, check, recurring, and IVR payments, as well as APIs that support standards-based integration. NIC Indiana’s solution is architected to support industry-standard REST APIs that provide options for integration into a variety of solutions and systems, such as kiosks and mobile systems. These APIs are core to the solution which ensures all of the data is consistent, secure, and available for all users.  Since the NIC Payment Platform uses modern APIs, middleware such as MuleSoft can easily be connected with the payment platform. For instance, MuleSoft could make calls to the NIC Payment Platform APIs as part of larger service orchestrations or MuleSoft could be used as an API gateway for the payment APIs to allow enterprise control and visibility of payment API calls. NIC Indiana has a long history at assisting third-parties with API integration and is confident in our ability to integrate with MuleSoft or other middleware solutions. In order to provide the highest level of service to the state, NIC Indiana has partnered with STLogics and their subsidiary, RadCube, in order to provide extensive experience with MuleSoft.  RadCube’s experience with MuleSoft allows NIC Indiana to offer a large array of services to the State of Indiana. Their MuleSoft experience includes more than just development, such as:   * Deployment planning and preparation * Proven frameworks to guide and accelerate implementations * Design and configuration * Workflow and business process improvement * Application and system integration * Mapping and data transformation * Testing and troubleshooting * Monitoring and support   NIC’s robust understanding of payments paired with RadCube’s expertise in MuleSoft will ensure the state receives a final solution that is stable, reliable, secure, and exceeds the expectations. |

* + - 1. The Contractor must provide an integration guide for its SaaS, PCI DSS compliant interface solution. Please provide examples of integration guides that have been created to meet the needs of customer of similar scope and complexity to the State. Please provide examples across the different types of State integration needs such as API, POS, Web, Virtual Terminals.

|  |
| --- |
| NIC has provided an example of the NIC-confidential and proprietary *CCP Integration Guide* titled *F.1 CONFIDENTIAL CCP Integration Guide*. This API library is used for communicating with our common checkout page for the state’s review. This document provides details and examples where appropriate for common scenarios for transactions and how agencies can utilize the proposed NIC hosted checkout page (CCP). The *F.1 CONFIDENTIAL CCP Integration Guide* contains NIC’s proprietary information and information that, on its own or in combination with other information, could be used to compromise the security of systems or to interfere with the normal operation of the system.  The NIC Payment Platform CCP is the PCI-compliant payment page that provides for configurable templates and elements to allow agencies to deploy payment pages quickly and easily with their logo, directional text, and other information while reducing programming and development costs. Instead, the agency will simply provide graphics and other configurable elements in a file and use a web services based API to call the payment page.  The NIC Payment Platform provides flexible integration capabilities, including API, point of sale, online (web), virtual terminals, kiosks, IVR, and more. In addition to this CCP API guide example provided, NIC provides documentation for our DirectConnect API to our government partners who wish to directly interface with the NIC Payment Platform, even though this integration method increases the PCI scope of the State’s service. |

* + - 1. The Contractor must provide a user guide for its SaaS, PCI DSS compliant interface solution. Please provide examples of user guides that have been tailored to meet the needs of customers of similar scope and complexity to the State. Please also provide examples of existing established user guides. Please include details on required timing to provide a tailored user guide.

|  |
| --- |
| NIC provides a well-documented set of user guides for our PCI DSS compliant SaaS administrative user interface that is configured to meet the needs of Indiana agencies. NIC provides these guides as a standard component of the configuration and launch of the NIC Payment Platform.  Please refer to the *F.2 CONFIDENTIAL CCP User Guide* for an example comprehensive user guide. CommonCheckout Pages, otherwise known as CCP, processes electronic payments online or at the Point of Sale without building, hosting, or maintaining payment pages within a Government’s environment. CCP provides several advantages including ease of integration to applications, PCI compliance achievement, duplicate prevention, configurable receipt options, and a customized look and feel for payment activities. CCP offers 200 configurable elements to customize the look and feel of the webpage and collect the desired data from your payer. Each agency can have their own separate payment pages that integrate seamlessly with an online or cashiering application. CCP integrates with the NIC Payment Engine for payment management and reporting. The solution also allows for configurable options for receipts and end user management. Using the CCP interface, our solution ensures no sensitive payment information is ever stored locally on any hardware and also ensures no sensitive cardholder data is transmitted over the government’s network.  *F.2 CONFIDENTIAL CCP User Guide* is a comprehensive user guide that addresses the following topics in detail:   * Introduction to Views * Skin Set Up * Skin Examples * Technical Set Up * Configuration in TPE * Fees and Payments * References and FAQ   As we complete the platform installation and configuration, NIC Indiana will initialize our support and training programs. We will compile documentation, prepare guides, develop training materials, and establish a training schedule for initial training of agencies on the use of the implemented NIC Payment Platform. Support will be provided as agencies are onboarded and will be provided ongoing for the duration of our contract. |

* + - 1. The Contractor must provide a solution that provides the services and functions for validating, accepting and processing payments to include but not be limited to the types listed in Attachment J- Scope of Work Section 1.4.3.1.(1).(ii).(1) and Attachment K- State Entity User Requirements. Please include any special requirements or considerations needed for all services or functions listed, specifically holds and blocks. Please detail your current offering and describe your ability to meet all requirements listed.

|  |
| --- |
| The NIC Payment Platform was built specifically for the needs of government and has evolved over two decades of real-world usage to be the most functional and reliable payment processing and financial management technology available to government. The NIC Payment Platform is hosted in high-availability, high-security datacenter facilities operated by Evoque (formerly AT&T) and administered by NIC. PCI DSS Level 1 compliance is maintained for both the hosting environment and the payment software itself. All payment processing for Indiana will use the NIC Payment Platform gateway, including processing of credit card, debit card, and e-check (i.e., ACH) payments through online, IVR, point of sale, mobile, and alternate payment channels. The NIC Payment Platform offers flexible and configurable integration methods to ensure maximum utility, provides the necessary gateway and connections to merchant processing services to fuel the transactions, and the enhanced visibility through reports and reconciliation tools to allow agency payment experts to manage the entire lifecycle of payments.  NIC is proposing to deliver payment services to Indiana as a Payment Facilitator, leveraging one of our acquiring relationships with service provider, Fiserv. Unlike traditional processors or solution providers, this model will allow NIC to be fully responsible for all aspects of the process to include merchant boarding and underwriting, processing, settlement, disbursements, tokenization, refunds, chargeback management, transactional reporting, security, compliance, innovations, and more.  Payment Platform Capabilities  NIC Indiana is offering Indiana a flexible, configurable, modern, highly secure, PCI DSS compliant proven suite of payment technologies, which consist of the following modules:   * Centralized NIC TPE® Payment Engine gateway, administration, settlement, disbursement, and reporting module * Over-the-Counter (OTC) module for Point-of-Sale transactions * Common Checkout Pages (CCP) module for customized online web payment pages * Customer Database (CDB) module for billing and recurring payments * Prompt Pay module for SMS and email-based payments for citizens * OnTheGo® Pay module for taking POS credit and debit card payments on a mobile device in the field * Wallet that streamlines government mobile payments * Fiserv CheckFreePay offers the ability to accept cash through Fiserv’s CheckFreePay agent network   Alignment with Attachment J  The NIC Payment Platform is a proven enterprise-level solution, specifically designed to provide government, citizens, and businesses a secure and reliable ecosystem to conduct e-commerce activities, including the features listed in *Attachment J- Scope of Work Section 1.4.3.1.(1).(ii).(1)* and *Attachment K- State Entity User Requirements*. The solution provides a proven, single integrated service to manage end-to-end payment management for Indiana, including all payment types and all channels. Our system can scale from a single low-volume service to supporting high-volume, enterprise payment processing for entire states.  The NIC payment Platform supports or will support the following payment processes and types:   * Authorizations * Holds * Settlements * Full or partial refunds, including ACH credits * Credit cards (Visa, MasterCard, American Express, and Discover) * PIN-based or PIN-less and Signature debit cards * Major debit networks * Electronic checks, including ACH debits and guaranteed electronic checks * Gift Cards * POS/In-Store * Acceptance of both swipe and key entry * Acceptance via PC/Workstation with USB or like swipe * IVR/Pay by Phone * Mobile Payment * WEB/Online Entry * Integration into third party and state applications * AdHoc form creation followed with payment processing through NIC Indiana’s low code platform * One-time ACH payments and recurring ACH payments over the WEB and IVR * Transaction status * Heart beat/system checks * Split payments over the counter, with split payments through CCP in development for a future release * PayPal * Venmo in a future release * Apple Pay * Amazon Pay * Visa Checkout and Masterpass are in development for future implementation * Google Pay contactless payments * Pay with my Bank * Retail Cash * Samsung Pay * Text Payment * QR Code Payment * Voice Payments with Amazon Alexa through Amazon Pay * Payment Disbursements   Holds and Blocks  The NIC Payment Platform is configurable to include an authorization/capture process that can complete a credit card transaction in two steps. If enabled, the NIC Payment Platform will perform an authorization/hold on a credit card to verify the funds are available. If the authorization is successful, the integrated agency application can then initiate the backend processes that complete the transaction in their system, then make a capture call to the Payment Platform in order to complete the transaction. This provides added flexibility to the government partner, and often streamlines the checkout process in systems that offer eCommerce or capturing of funds after a specific action has taken place (e.g., record mailed to citizen).  Similar to the platform’s duplicate blocking capabilities, the NIC Payment Platform also has the ability to block customers from leveraging the same payment method in the event of unwanted transaction behavior. The payment platform can either allow for an agency administrator to selectively block and unblock a customer from continuing to leverage a specific payment method for future transactions, as well as establish an automated business rule specific to failed payment attempts. NIC will work with the State to determine which method is preferred and to configure the business rule to adhere to the State’s desired outcome. This may include factors such as how long the block is in place, if it is for a specific service or the state as a whole, and whether a State authority has the ability to remove the payment method from the blocked list. |

* + - 1. The Contractor shall process each transaction in real-time, unless otherwise agreed to, and in accordance with all requirements listed in Attachment J- Scope of Work Section 1.4.3.1.(1).(iii). Please detail your current offering and describe your ability to meet all requirements listed. Please include specific details regarding the batch and settlement processes. Do you have the capability to batch and settle debit and credit transactions together? What system, process, or reporting offerings enhance the efficiencies of the batch/settlement/deposit reconciliation process?

|  |
| --- |
| The NIC Payment Platform provides enterprise class financial management technology to government partners across the U.S. and is an industry-proven, reliable, secure real-time transaction processing solution. The state-of-the-art payment engine also provides real-time transaction research and online reporting tools for managing transactions occurring in real-time.  Batch & Settlement  The NIC Payment Platform includes a robust disbursement engine, that is designed specifically for government. Settlement of funds starts with establishing the proper hierarchical structure of merchants and services within the platform. There are a variety of configurations that can accommodate each state agency at an agency or specific service level. For instance, there are many cases when an agency prefers or requires disbursing funds for a specific service to a separate bank account in comparison to another unrelated service within the same agency. Likewise, a specific service may require funds collected in a transaction for a specific item to be deposited into a different account than another item on the same order. All of this is made possible through NIC’s disbursement engine capabilities.  In addition to an interactive transaction, the platform is also able to prevent activities such as, duplicate file postings, out of balance, and missing files through a variety of standard controls that are in place. Files are created with a timestamp such that no two files with the same name are duplicated. As the NIC Payment Platform creates the batches that transmit the disbursement files, our file creation job balances the expected disbursement amount and file count with the settlement files sent from our processor. If these do not match an exception report is sent to our Finance team for research. NIC Payment Platform jobs are monitored, and an alert is automatically sent to our service desk if the files are not properly generated.  Alignment with Attachment J  The proposed NIC solution provides the ability to accept, validate, and process the requirements set forth in *Attachment J- Scope of Work Section 1.4.3.1.(1).(iii)*, “Payment Processing.” The NIC Payment Platform meets all of these requirements today in our Indiana implementation, and specifically provides the following features to meet the stated requirements:   * The NIC Payment Platform supports file transfers via Secure File Transfer Protocol. * Provide the ability for the customer or user to print and email a receipt which contains the required information and can be customized to the needs of the State Entity. * Includes the provision, management, and support of payments through all required channels (POS/In-Store payment processing, IVR/Pay-by-Phone, WEB/Online Entry, Mobile Payment) and can support other agreed to methods for completing credit card and e-Check transactions. * NIC Indiana can provide a toll-free IVR, upon request, for applicable services. * NIC Common Checkout Page hosted checkout pages enables all user applications to accept cardholder data off the State network with redirection of the user back to the calling application when complete. * The platform is certified to provide end-to-end encryption for applicable services and has a series of Listed P2PE solutions available on the platform. * The NIC Payment Platform includes comprehensive disbursement and settlement functionality to direct funds to the State depository designated by the State Treasurer or as outlined in an approved, State Entity SOW. * The platform can deposit funds into multiple accounts as designed by the State meeting deposit timeframes and other requirements as mandated by the State Board of Accounts State Agencies Manual. * The platform allows for multiple settlement accounts through the use of SKUs or “settle codes” with disbursement rules to determine the appropriate settlement and these SKUs can be configured to the specific needs of each State Entity. The NIC Payment Platform has the ability to add customizable SKUs to each item in a single transaction. This means an unlimited number of tax and/or fee payments with unique SKUs can be added to the order, so the user can make a single payment when purchasing multiple items. On the backend, our disbursement engine can send the funds collected to various destination accounts based on the disbursement rules for each unique SKU. * The platform has the ability to batch transactions on a manual or scheduled basis and adjusts batch processes based on time change events. * The system provides real time notification, where applicable and as requested, of the submitted payment so that the customer and/or user can (1) see that the payment was successful or (2) read a failure message explaining the issue and/or (3) be notified of a pending status if it should remain in pending status according to service setup. * The system creates a payment transaction log record for each payment when the customer and/or user attempts to make a payment which is updated when confirmation of authorization or rejection is sent back from the processor. * The NIC Payment Platform can process multi-million-dollar payments without multiple payment transmissions, as allowable by the acquiring bank. * Includes robust fraud prevention including duplicate payment prevention rules to help prevent duplicate payments. * The platform provides a confirmation number back to the State after completion. |

* + - 1. Please provide details on the different options State Entities will have relative to signature capture during the transaction process. Please include samples where applicable.

|  |
| --- |
| NIC Indiana POS devices provide signature capture capabilities through the Ingenico Lane series of devices and the NIC OntheGo® mobile payment solution. The Ingenico Lane 5000 and 7000 devices support direct signature capture using the device screen and a stylus.  The following image shows signature capture for the Lane 7000 and 5000 devices.    The NIC Payment Platform holds a level-3 certification to leverage the Ingenico Lanes Series devices for EMV/Chip Reader transactions. All terminals in the series are certified to support contactless payments, EMV, and PIN.  In addition, the NIC OntheGo® Pay solution allows users in the field to capture signatures directly on their mobile device when processing payments from their mobile device. |

* + - 1. The Contractor must, at its own expense, ensure that all current applications processing payments must integrate with the Payment Processing Solution it is proposing as part of this RFP response. A listing of current applications can be found in Attachment K- State Entity User Requirements. Please confirm your understanding and describe your ability to fulfill this requirement.

|  |
| --- |
| NIC Indiana understands and ensures that all current applications provided in *Attachment K* can integrate with the proposed NIC Payment Platform solution. NIC Indiana can attest that the proposed solution currently integrates with many of these applications and is providing payment processing services for these State Entity Users today. Furthermore, we have analyzed the functional requirements for services listed in *Attachment K* that are not currently processed through the NIC Payment Platform today and are confident that these services can be adapted to process payments through our platform with minimal effort. |

* + - 1. Please describe your company’s abilities and offerings within APIs such as, but not limited to, lightboxes, customization, confirmations, validations, direct end user back to the State Entity site. Please provide examples from Contractor customers of similar scope and complexity to the State of Indiana.

|  |
| --- |
| State of Indiana participating agencies have the option of leveraging either NIC’s fully hosted Common Checkout Page (CCP) solution or a direct connection to NIC’s gateway to link state web applications with the NIC Payment Platform. In the hosted CCP method, the end-user selects “Pay Now” from the state’s web application and then they are transferred to NIC’s fully hosted checkout screens that are part of the NIC Payment Platform.  When using the hosted common checkout page, this process consists of a redirect, as well as API calls to prepare the system for the order and to monitor for details, such as order status, failures, etc. Upon completing the checkout process outside of the State’s network, the customer and payment information is processed through the Payment Platform Gateway for authorization and collection via the merchant processor.  The figure below illustrates the payment flow for web applications.    The fully hosted CCP module allows Indiana to limit its scope in PCI, while re-directing the end-user to NIC to collect sensitive regulated payment details. The module also provides co-branded experience, a mobile responsive HTML5 view, as well as an inline iFrame and a view specifically designed for cashiers to leverage card present devices and in-person transactions. CCP can either be a redirect or can be used within an iFrame.  Following is an example of a state government partner’s use of NIC’s hosted checkout page. The example below also highlights the system’s customization capabilities to brand the checkout page, even allowing branding within a merchant hierarchy to give the government the ability to do branding at the state level, the merchant or agency level, and/or the service level.    The following screen shot shows an example of the online confirmation page received by the customer. This page shows the same language as the online payment screens.    For scenarios where the State agency would prefer not to redirect the customer to NIC’s common checkout, then the state web application would present a checkout page to the user and leverage the DirectConnect API to pass customer and payment information to the gateway for processing. This method increases the state entity’s PCI DSS related responsibilities, though, as the web application will be exposed to cardholder data. |

* + - 1. Please describe the mechanisms your company utilizes to stay at the forefront of the payment processing field in terms of different processing types and services offered. Please provide an example of the research, development and deployment undertaken by your company to integrate a new payment processing type with a customer. Please list any offerings currently available that are not required in this RFP.

|  |  |  |
| --- | --- | --- |
| Customer-Driven Innovation  The NIC Payment Platform technology has been installed, expanded, and continuously enhanced for 20 years. Through relationships with 32 state partners, 7,800 agencies, and thousands of local entities, NIC’s greatest sources of innovation are our customers and the citizens that rely on their transaction-based services. Our customer-driven innovation approach to product expansion and improvement allows us to invest in e-commerce and card present initiatives by looking through the lens of our government partners.  NIC’s customer-driven innovation puts governments’ needs at the heart of our R&D approach. Out of necessity, NIC long ago realized that traditional, insular methods of innovation — developing new products in-house in a vacuum — do not always reflect our government customers’ actual needs and desires. Thanks to our organizational approach of embedding project delivery teams with our government partners, while centralizing NIC Payment Platform product development, we have on-the-ground understanding of exactly who our customers are, what they need, and the challenges they need our expertise to solve. In the NIC customer-driven innovation approach, our frontline digital government experts, who are informed by government partners, are at the center of driving innovation to the NIC product suite. Simply put, customer-driven R&D propels the innovation effort away from headquarters and out to those closest to the government customer.  In addition to our customer-driven innovation approach, NIC leverages our active participation and research of industry associations as well as changing legislation across the U.S. NIC and its affiliates have cultivated relationships with an extensive list of technology-specific organizations. Specifically, we closely follow and engage in organizations such as the PCI Security Standards Council, NACHA, (ISC)2, Gartner,), National Association of State Budget Officers (NASBO), and NASCIO to name a few. NIC also has relationships with technology and payment leaders such as Visa, MasterCard, American Express, Discover, Amazon, Microsoft, Google, Apple, Fiserv, WorldPay, ECHO, Intuit, PayPal, Bank of America, U.S. Bank/Elavon, Wells Fargo, Santander Bank, Western Union, and IVR providers such as Twilio and Vail. These relationships allow us to be prepared for industry changes such as new versions of PCI DSS, NACHA changes, and new technology and services as they emerge for payments. NIC Indiana communicates internally using NIC’s collaboration platform and is able to communicate with NIC technical experts across 32 states to understand what our customers want from the next generation of payment services.  R&D Example  In the last ten years governments have witnessed a revolution in e-commerce, signaled by the online retail commerce revolution, which has disrupted traditional government payment channels and the basic government-to-citizen relationship. Like online retail predecessors, governments can distribute, promote, and sell services online, with a secure, flexible e-commerce platform providing the foundation for nearly every transaction. With the ever-increasing shift to the e-commerce model, governments see increasing pressure to deliver commercial-grade e-commerce solutions that wrap innovative digital government services.  One important, real-world example of NIC’s ability to determine a market need, research the problem, develop and test a comprehensive solution, and integrate that solution within our Payment Platform is the ***OnTheGoÒ Pay*** mobile payments app.  While working with the State of Idaho, NIC and the State recognized that not all government business takes place in the office. And Idaho’s vast rural landscape often does not support data connectivity for instant payment processing on mobile devices. So, when public safety officers or tax collectors are in the field, they were often without an affordable, secure, reliable way to take electronic payments.      To remedy the connectivity issues, ***OnTheGoÒ Pay*** goes beyond run-of-the-mill mobile device payment processing by combining the importance of security with the flexibility of true “store-and-go” capability. The app’s value lies in its ability to encrypt and save pending transactions until the device is within range of a service area or Wi-Fi network, when the app will automatically process.  The app takes advantage of mobile technology to untether payment processing from a walk-in government office. With ***OnTheGoÒ Pay***, secure citizen–to-government payments can now take place remotely on tablets or smartphones. The technology opened up a new dimension of face-to-face customer service for citizens.    ***OnTheGoÒ Pay*** has the ability to allow government entities to pass on the credit/debit card processing fees to customers. In Idaho, NIC retains the fees and electronically deposits the statutory funds into the pertinent government agencies' bank account.  Added Value Offerings  In addition to the proposed payment services in response to the RFP requirements and OntheGo***Ò***  Pay, the NIC Payment Platform integrates with multiple, innovative solutions that are deployed for governments across the U.S. and also available to the State of Indiana. Additional payment-related applications and services include:   * Prompt Pay module for SMS and email-based payments for citizens * Gov2Go® Pay digital wallet that streamlines government payments * Fiserv CheckFreePay® offers the ability to accept cash through Fiserv’s CheckFreePay agent network   NIC Prompt Pay  Launched in Idaho, NIC’s Prompt Pay allows government entities to send payment links to customers via SMS text and email. Prompt Pay features a dashboard interface for government personnel to enter how much the customer needs to pay, along with a description of what the payment is for. After the payment information is entered, a government employee can send a link to the customer’s mobile device by text, or to their email address, or both. The customer can then use the link to pay the government service by entering their credit card or checking account information, thus removing the government entity from Payment Card Industry (PCI) scope.   |  |  | | --- | --- | | **Browser Example** | **Cell Phone Example** |   Prompt Pay takes government entities out of PCI scope by allowing customers to enter their respective credit card information on their own devices or computers. Government employees and systems are removed from exposure to credit card data. Prompt Pay uses NIC’s secure processor for Visa, MasterCard, AMEX, Discover and electronic check payments.  NIC Wallet API  Front-end applications can implement credit card management and payment processing features without exposure to PCI data. PCI data is submitted via iFrame views delivered to the end user browsers from a web application that works in coordination with the Wallet API to collect and store the user’s payment information in NIC’s secure PCI vault. Once the payment information is stored in the vault, then the calling application is provided with a token to identify the payment method to be leveraged for future transactions. This makes front-end applications easier to design, build, maintain and update without impact to the payment processing component. The reliability, security, and ease of integration of the Wallet API allows the front-end application to define user interaction.  Wallet API works with the client’s existing authentication method to provide stored payment methods. No authentication is required for one-time non-saved payment processing.  Benefits Include:   * Removes Risk and Liability * API Integration * Reduces development time and cost * Account Management * Uses stored or non-stored payment methods * PCI DSS Compliant   Citizen Experience Platform  If the agency prefers a more integrated approach for mobile payments, then the calling application can re-direct the user to NIC’s common checkout, where the user would make their scheduled or one-time payment selections that are available for that specific application. The scheduled and recurring feature is not enabled by default, so this would be configured with the agency when establishing the payment service for each specific application.  When utilizing the fully integrated approach, NIC will leverage our Citizen Experience platform, Gov2Go®, to manage the user authentication to access their stored payment methods, as well as manage and edit their current selections. The calling application will leverage the fully hosted common checkout to provide the details of the transaction to NIC and NIC will leverage a postback method to provide the calling application with details of the payment setup, schedule, updates to a schedule and notification of a payment made for each instance.  CheckFreePay  NIC has partnered with Fiserv to provide NIC's government partners with access to the CheckFreePay agent network through NIC's integrated payment processing platform. In this case, the customer remits all funds in cash to the retail agent location, including the proposed service fee. Once the cash is collected from the user, then the transaction is completed in the NIC Payment Platform and disbursed to the specific government agency account two business days after the transaction.  There are almost 400 retail agent locations in Indiana, such as Wal-Mart and Kroger that provide a cash payment acceptance channel to the unbanked and underbanked residents. |

* + - 1. Please provide details and examples of Gift Card Program offerings your company has implemented for other governmental customers either statewide or for individual State Entities. Include implementation requirements and time frames with your response.

|  |
| --- |
| NIC Indiana has assisted the Indiana Department of Natural Resources with electronic gift cards for their online hunting, fishing, and trapping solution for numerous years. Customers are able to purchase gift cards online, and recipients are able to redeem their value within their online profile for use on future purchases. The gift certificate processes are built into our shopping and checkout module within the application.  Additionally, NIC Indiana can work with our third-party provider to provide closed-loop stored value cards. Our partner is the largest provider of closed loop gift cards in the US and can provide gift cards with the ability to load funds and use those funds for transactions and provide for activities such as balance inquiries.  NIC is partnered with Fiserv, who holds 55% of the gift card market share with more than 350 national and global gift card clients from brands that everyone knows. Fiserv has been a leader in this space for more than 26 years and processes more than 12B gift card transactions annually.  Based on the platform’s direct integration with Fiserv, the platform would be capable of delivering a closed network gift card solution to Indiana within months, not years, of solidifying the programs requirements.  Together as a partnership, NIC Indiana would like to learn more from the State about the use cases for the closed network gift card program. This will support implementation decisions for e-Commerce vs Card Present, dedicated gift card portals, virtual or hard issuance, and more. |

* + - 1. The Contractor must provide to interested agencies Point of Sale (POS) acceptance of swipe, key entry, and wireless pay for completing credit card transactions. The Contractor shall provide equipment and/or software, including terminals, EMV-capable integrated terminals, key pads or alternative devices necessary to process card transactions at the merchant/sales locations. Wireless, Mobile and Tablet POS equipment shall offer both wireless and cell signal functionality. Respondent shall offer POS equipment that is compatible across a variety of specific carriers (*e.g. Verizon or AT&T)* and/or be operational with specific generations of broadband cellular network technology. The Contractor shall have the ability to provide printers, ink, and paper upon request as necessary. POS equipment shall have the ability to process full or partial refunds at the terminal level through manager provided override or password functionality. All POS equipment shall have back up capabilities to process and retrieve transactions in the instance of events such as power loss or internet connectivity issues. Device ownership and maintenance is to be provided by the Contractor at no additional cost to the State. The Contractor’s Payment Processing Solution must have the ability to install and support Point-of-Sale Equipment Terminals in State-designated locations at no cost to the State. The State desires a Point-to-Point Encryption (P2PE) compliant solution. A list of P2PE solutions can be found on: https://www.pcisecuritystandards.org/assessors\_and\_solutions/point\_to\_point\_encryption\_solutions.

The State also desires PCI Approved PTS Devices. Please list name of devices being offered through this RFP as found on: <https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices>

Please describe your ability to meet these requirements. Please detail which specific carriers and broadband technology are supported by your POS equipment. Please include process details for terminal level refunds, including screen shots. Please describe the backup capabilities offered to process and retrieve transactions in the instance of events such as power loss or cellular/internet connectivity issues. Include details on the storage of and access to POS transaction data. How are transactions processed in the event of a cellular or wireless connectivity issue?

|  |
| --- |
| NIC Indiana understands, will comply, and is acutely aware of the POS requirements across the State. Point-of-Sale (POS) has many different implementations and use cases across the government landscape. NIC has focused its in-person or face-to-face offerings around providing a suite of task specific hardware that integrates with NIC’s software to continue to stand by our efforts to minimizes PCI and device integration burdens to the government. The hardware ranges from simple encrypted swipe devices to fully featured and Validated Point-to-Point encrypted contactless and EMV payment devices. If an agency already has a POS software solution that is responsible for all the back-office functionality, NIC has architected our solution to tether to your host PC via USB and will conduct all communications through an NIC built and managed software client. This client provides the POS software with the option to leverage an API for direct connection for a more integrated approach, as well as the option to leverage NIC’s fully hosted common checkout platform to manage the device communications with minimal POS system integration. As such, NIC’s solution provides the ability to process full or partial refunds at the terminal level through manager provided override or password functionality within the Payment Platform.  In addition, it is important to note that all POS transactions are processed through the NIC Payment Platform and therefore all reporting, reconciliation, or end-of-day tasks are managed by the same system as all other payment channels. There is no need to run separate close-out functions or take action on each individual terminal at the end of your day. These functions are instead the responsibility of the NIC Payment Platform. The result in a robust payment management solution for each of the state’s payment implementations with NIC that provides our government partners with the power to manage their payments as needed for their specific business purposes.  The proposed Ingenico Lane 3000, 5000, and 7000 series of devices are all listed as PCI Approved PTS Devices and can be found on the PCI SSC website provided in the RFP by the State. The NIC Payment Platform holds a level-3 certification to leverage the Ingenico Lanes Series devices for EMV/Chip Reader transactions. This series starts with a small form factor device called the Lane 3000 that is comparable to the size of a smart phone and scales up to the Lane 7000 devices, which is found at many major big box retailers. The larger device provides a rich color display that can be used for presenting form-based screens to a user at the time of checkout. All terminals in the series are certified to support contactless payments, EMV, and PIN.  Wireless, Mobile, Tablet POS  NIC’s mobile technology solutions align specifically with the requirements of the RFP. For example, with OnTheGo® Pay, cashiers can use an encrypted MagTek device connected to any smart phone or tablet, and process payments in remote areas or small offices. OnTheGo Pay is a payment application downloaded on any smartphone or tablet and can work using a wireless network or a cell signal using a SIM card. OnTheGo Pay also has “store-and-forward” capabilities to take offline payments and process them once the device is either in cellular or wireless range.    In addition to the innovative OntheGo product, NIC is continually looking for ways to increase its hardware product catalog for our partners. The following mobile-specific products are either being actively integrated or are on a future roadmap to be added to the NIC Payment Platform catalog.  Ingenico Link 2500 Series  Featuring a pocket-sized, light weight and slim design, the Link 2500 has Wi-Fi and Bluetooth capability to connect to any iOS, Android or Windows-based tablet or smartphone.    Ingenico Moby 5500  The Moby/5500 is compact card reader that accepts all transaction types including EMV, magstripe and NFC/contactless payments. It is compatible with iOS, Android, and Windows, and connects easily via Bluetooth with over 500 iOS, Android, and Windows smartphones and tablets. |

* + - 1. The Contractor must make Virtual Terminals and Standalone Platforms available to interested agencies for completing payment processing transactions. Please describe your ability to meet these requirements.

|  |
| --- |
| NIC’s payment solution has a “virtual terminal” component that allows agencies to take payments manually without the customer present. The services and input fields necessary to collect the payment information are configurable through a back-end administrative interface. All configurable fields and checkout pages are web-based and fully hosted in our PCI Level 1 compliant card data environment.  NIC has two lightweight virtual terminal offerings. Both offerings share common cashier recording features such as the ability to log incoming paper checks or cash, in addition to processing digital payment types like credit or debit cards. Each of the offerings also integrate with an encrypted keypad to help mitigate key logger concerns from malware. The differentiator between the two offerings is that one can be stand-alone from any other calling application or POS system and the other is an integrated version of NIC’s hosted common checkout. |

* + - 1. The Contractor shall provide routine and non-routine servicing and maintenance of POS equipment at each location on conditions and terms to be mutually agreeable to the Contractor and the State. The Contractor shall reprogram existing equipment to ensure compliance with any current State or federal laws or industry standards as well as any laws or standards that may be set forth at a future time. The Contractor shall provide technical support and troubleshooting help for the State’s existing and future equipment. The Contractor shall replace non-functioning or broken equipment, when applicable, and serve as the State’s advocate when handling equipment issues with the manufacturer. In the event of an equipment malfunction the Contractor shall repair or replace the malfunctioning equipment on-site within forty-eight (48) hours of receipt of notification from the State Entity. Please provide details of your company’s current process for monitoring, maintaining, and updating POS equipment and software. Please include notification procedures and communication requirements. Please include details on the process to return non-functioning or broken equipment at the Contractors expense.

|  |
| --- |
| NIC Indiana understands and will comply with agreed-upon conditions for servicing and maintaining POS equipment at each location. NIC and its proposed subcontractor will provide technical support and troubleshooting for the State’s current and future equipment, as well as replacement of broken or malfunctioning devices, as required.  NIC Indiana in coordination with the state’s ticketing system, vFire, tracks device maintenance, replacements and repairing non-functioning or broken equipment. One example for monitoring, maintaining, and updating POS equipment and software is specific to the BMV branches throughout the state. When a device is no longer working as expected, the branch will submit a ticket using vFire that is routed to a technician through IOT. Once a technician has completed a full diagnosis of the machine and determines it needs to be replaced, the ticket is updated with the issue details and routed to NIC Indiana with the request for a replacement device. NIC Indiana pulls the details about the defective device and updates an inventory log of over 1200 devices outlining the problems of the defective device. NIC Indiana then ships a replacement device to the branch manager along with a return label to have the defective device mailed back to NIC Indiana. Once the defective device is received from the branch, NIC Indiana then sends the device to the support team, Verifone, to have it refurbished. The device support team sends the refurbished device back to NIC Indiana. NIC Indiana then updates the inventory logs to include the fixed device with the pool of replacement devices. NIC Indiana updates the inventory logs on a daily basis and will send a replacement device within 24 hours of the ticket being assigned to NIC Indiana. Additionally, NIC Indiana keeps a close eye on the number of replacement devices available and will order more devices when supply levels hit a defined inventory threshold. NIC Indiana is also responsible for sending replacement stylus pens, MagTek Swipe Devices, and more to ensure POS locations throughout the state are able to maintain operations. |

* + - 1. Contractor must accept responsibility for setting up, in its own name, merchant accounts for each application that requires and/or permits the collection of fees from State users, whether the application is developed by the Contractor, its Affiliates, or by a third party. The Contractor is responsible for all fees associated with merchant account maintenance and support as well as merchant fees for payment processing (to be invoiced to the State), collecting convenience fees and additional fees as requested by the State, chargebacks and all other transaction-related expenses, excluding statutory fees which will be reimbursed by the State if the Contractor receives a chargeback after payment. The Contractor's Payment Processing Solution must provide the ability to set up merchant accounts for each application that requires the collection of fees from State users. For each merchant account set-up, the Contractor must provide to the Payment Processor the transaction data required to complete the authorization and capture of credit card funds. Please provide a description of the approval process, including time frames and communication flow, for the setup of merchant accounts. Processes should be defined for both new account set up and account modification throughout the life of the contract. Please include an example of the documentation that will be supplied to IOT and the State Entity upon completion of each merchant account set-up instance. Please outline the expected deliverable timeframe for merchant account set up and delivery of the accompanying documentation. Please confirm your ability to meet these requirements including details on the number of merchant accounts managed at any single customer simultaneously.

|  |
| --- |
| NIC Indiana understands, will comply, and confirms that the proposed solution will meet these requirements, including details on the number of merchant accounts managed at a single customer simultaneously.  As a Payment Facilitator, NIC can provide an unlimited number of merchant numbers and terminal IDs to meet the State’s processing needs. NIC will acquire these merchant accounts with our third-party merchant acquirer and configure the accounts in the Payment Platform. Additionally, the NIC Payment Platform is designed to support multiple layers of merchant hierarchy and service identifiers to support the State’s processing and reporting needs, which might not always require separate merchant numbers.  The hierarchy-based structure of the NIC Payment Platform will allow NIC to build out the payment solution based on how Indiana agencies are structured. Each payment service will be configured based upon merchant account, service type, payment channel, and fee structure. The hierarchy is flexible and scalable, allowing adjustments and additions to services and merchants. There is no limit to the number of merchants and services in the merchant hierarchy.  The NIC Payment Platform can handle multiple web applications using one merchant account or a one-for-one merchant account to application configuration. Typically, the necessity of separate merchant accounts is driven by the need for unique descriptions on the end-user's credit card statement. For reporting and reconciliation purposes, the system can be configured with a hierarchy based on the State’s own reporting hierarchy.  NIC will work as a consultant with the State during the implementation of the project and on-going when boarding State Entities to guide these decisions.  Merchant Account Setup Process  Once the initial hierarchy and foundation are established, NIC uses a standard approach for onboarding each agency and service. This process includes discovery with the agency and appropriate stakeholders to understand the payment processing options that will be required. This discovery process drives additional provisioning workflows, such as merchant boarding activities, sub-merchant agreements, American Express boarding, ACH setup, etc. The attached file *F.3 Service Code Setup Template* provides a template to gather all the necessary information in order to setup a new service code in TPE. Once the document is updated with the correct requirements for the agency's service code, the document is circulated for initial approval signatures, the work to set up the service code is completed, it is tested, and the document is circulated again for deployment approval signatures. Once all of these steps are completed, NIC Indiana sends the fully signed/executed document to IOT and the agency also gets a copy.  On a per service basis the NIC team will also configure NIC payment platform setup and configurations. This includes financial testing workflow, where an end-to-end “penny test” will be performed for each settlement account NIC adds to the platform. Once financial testing has occurred for an account, other services can leverage this account for settlement without additional testing, streamlining on-going integration of services that make use of the account.  Most new payment methods, such as a state entity expanding from credit card and debit cards to now include ACH is a simple configuration change on the platform. This rapid timeline is also the case when adding a new service under an existing agency participant hierarchy on the platform. As a nod towards efficiency, the NIC Payment Platform supports the use of soft descriptors to allow for the same merchant ID to be leveraged for certain eCommerce implementations, cutting out the time for new merchant ID issuance in many cases.  Merchant Account Setup Timeframe  To obtain a new merchant ID it can take 10-21 calendar days which is based on timing from the acquirer, American Express, and the various onboarding processes that are managed by NIC. Once the merchant ID is setup and testing is completed, NIC Indiana circulates the documentation for approval signatures to push the service to production. After the document is fully signed, a copy is provided to IOT. |

* + - 1. The Contractor must distribute funds collected by it on behalf of the State as set forth below and consistent with instructions from the Treasurer of State and in conformance with Ind. Code § 5-13. The Contractor shall have the capability to deposit funds into multiple accounts as designated by the State. All payments remitted by credit card users, including additional fees set by the State, shall be deposited directly into the designated Contractor-owned non-interest-bearing bank account as identified in the associated merchant account set up by the Contractor. All payments remitted by EFT users, including additional fees set by the State, shall be deposited directly into the State's designated bank account. The Contractor shall have the capability to deposit funds into multiple accounts as designated by the State meeting deposit timeframes and other requirements as mandated by the State Board of Accounts State Agencies Manual, the most current publication can be accessed at: https://www.in.gov/sboa/4447.htm Upon request the Contractor shall provide a daily flat file to be used for reconciliation purposes The Contractor must assist the State in the effective disbursement, to State accounts, of revenues received. The cut off time for transactions shall be agreed upon by the Contractor and State Entity for each individual Scope of Work. Please confirm your understanding of the requirements outlined in RFP Scope Section 1.vi and provide an example of the monthly payment statement. Please include examples of your company’s ability to provide flexibility for cut off times across a similarly diverse portfolio of payment processing needs.

|  |
| --- |
| NIC Indiana understands, and the proposed NIC Payment Platform solution complies with these requirements and those set forth in RFP Scope Section 1.vi. The proposed solution is currently configured in Indiana to meet these requirements.  The Payment Platform includes a robust disbursement engine, that is designed specifically for government. Settlement of funds starts with establishing the proper hierarchical structure of merchants and services within the platform. There are a variety of configurations that can accommodate each state agency at an agency or specific service level. For instance, there are many cases when an agency prefers or requires disbursing funds for a specific service to a separate bank account in comparison to another unrelated service within the same agency. Likewise, a specific service may require funds collected in a transaction for a specific item to be deposited into a different account than another item on the same order. All of this is made possible through NIC’s disbursement engine capabilities.  Based on the configurations, the NIC Payment Platform will set an effective funding date for each transaction at the time of successful capture. On the configured effective funding date, the system will batch the transactions and create and transmit a NACHA file to the bank for processing and depositing to the Agency accounts. Each day’s settlement reconciliation files can be delivered via SFTP or accessed any time online to support state agency integration into the State’s ERP system and reconciliation activities against bank transactions.  All payments remitted by EFT users, including additional fees set by the State, will be deposited directly into the State's designated bank account.  Additionally, daily settlement files from our processors are imported into the NIC Payment Platform and all transaction information post capture is recorded and tied back to the original transaction. This enables the solution to extract transaction information, including settlement dates, payment type batch ID’s, deposit amounts, summary by agency, chargeback data, return data and provides the State with a file that can be used to integrate with backend systems.  Reconciliation Tools  Each day’s settlement reconciliation files can be delivered via SFTP or accessed any time online to support state agency integration into the State’s ERP system and reconciliation activities against bank transactions. NIC provides real-time online reconciliation reports to authorized staff through our secure web-based reporting interface. These reports can be filtered in a multitude of ways including but not limited to custom date range, location, and payment type.  This information can also be used to create reports that match deposits to statements, match return and refund information to settlements and reconcile batches. Not only does this process save time in reconciliation but improves the efficiency of recording journal entries for the different services. The solution provides the ability to reconcile bank activity to each deposit daily.  Example Invoice Report and Monthly Statement    In addition to the Invoice Detail report, NIC Indiana provides an extensive invoice that includes a monthly breakdown of interchange, dues, and assessments for each Merchant ID. The following image shows a breakdown for one merchant ID from an invoice.    Ability to Meet Cut-off Times & Example  Cut off and batching of the state's deposit settlement is configurable for all payment types and transaction types. NIC Indiana can configure cut-off times in the disbursement profile on the hour mark. For example, one of our state contracts has a credit card cut-off time of 11:59:59 PM EST and an ACH credit card cut-off time of 7:59:59 PM EST. At least one agency has requested that the credit card cut-off time mirror the ACH cut-off time. Our engagement with DC Courts and Hamilton County, IN each have a 3:59:59 PM EST cut-off time. The NIC Payment Platform has been able to accommodate each of these custom cut-off times.  Cut off and batching of processor deposit settlement varies by processor, bank, and payment type. Processor cut-off time, bank cut-off time, and payment type are all factors influencing the Processor deposit settlement and may cause delays. |

* + - 1. As part of the distribution of funds, the Contractor is required to collect additional fees on behalf of the State as requested. (Please reference Attachment J- Scope of Work, Section 1.4.3.1.(1).(vi).(1). These fees are subject to change during the life of the contract. Please provide your company’s ability to collect, report and disburse this fee to the State and your ability to implement changes to the fee structure.

|  |
| --- |
| The proposed NIC Payment Platform solution meets these distribution of funds requirements defined in *Attachment J 1.4.3.1.(1).(vi).(1) “Additional Fees”* and is currently configured in Indiana to provide this functionality.  The NIC Payment Platform supports flexible configuration including data fields, merchant hierarchy, checkout user interface, types of payments accepted, how funds will settle, splitting transactions, and other business rules around reporting and disbursements. |

* + - 1. The Contractor shall submit an invoice, either electronic, paper or both, based on State Entity preference, to the State Entity’s Bill to Address, 35 days in arrears and no later than the 15th of the month. The Contractor’s invoice shall identify, at a minimum, the information listed below, and shall have the ability to customize based on unique requirements outlined in individual State Entity SOW’s: Contractor’s name and address that matches the Auditor of State’s records, invoice date, State Entity’s bill to information, business unit and/or service code, breakout of fees assessed, fee description and amount, transaction dates, chargeback date, transaction amounts, transaction counts, total dollar volumes processed, a breakout of fees collected, and invoice total. Please describe your company’s ability to meet these requirements. Please outline any quality assurance practices in place to ensure the accuracy of Invoices. Please outline the process in place for Invoice corrections, including time frame for resolution. Please provide examples of detailed Invoicing capability.

|  |
| --- |
| NIC Indiana understands and will comply. NIC will submit invoices to the Bill to Address, 35 days in arrears and no later than the 15th of the month, to individual State Entity’s, as outlined in each State Entity SOW. In accordance with the above-noted requirements, NIC will provide invoices with the following information:   * NIC Indiana name and address that matches the Auditor of State’s records * Invoice date * State Entity’s bill to information * Business unit and/or service code * Breakout of fees assessed * Fee description and amount * Transaction dates * Chargeback date * Transaction amounts * Transaction counts * Total dollar volumes processed * Breakout of fees collected * Invoice total   NIC Indiana follows very detailed steps, along with testing by both NIC Indiana and the State Entity to ensure the new service is setup correctly in NIC’s Transaction Processing Engine (TPE). After setting up the service code, NIC Indiana runs a test transaction to confirm the bank account is set up to and disbursing the funds properly. NIC will only enable a service for use after receiving confirmation that the merchant was setup and is disbursing correctly. When a new service is set to disburse to an already existing bank account that is set up in TPE, NIC Indiana will complete a test transaction in our User Acceptance Testing (UAT) environment to ensure the service is set up correctly to disburse to the correct accounts provided by the agency. Through following these quality assurance steps during the merchant setup process, the invoices pulled from TPE are accurate.  If a State Entity has selected to pay the merchant fees, NIC Indiana will bill the State Entity for that total merchant fee amount on a monthly basis. The agency is also provided a merchant report from the selected merchant processor (WorldPay or Fiserv) that is used to cross check the invoice sent from NIC Indiana. Following the proper steps to setup the new merchant account, ensuring the monthly merchant report is sent to the agency and pulling the invoice details from TPE are all required steps to perform quality assurance and ensure the monthly billing is correct. If any agency has selected to pay the transaction fees on behalf of the end user, NIC Indiana will net out the transaction fees per transaction.  A sample of a current invoice from NIC Indiana follows. NIC Indiana will update the invoice template to include all of the data fields requested by the State under the new contract.    The attached detail pages include a breakdown of total fees by Merchant ID and a breakout of the interchange dues and assessments for each Merchant ID. The following is an example of that breakout: |

* + - 1. The Contractor shall provide monthly Disbursement Reports to the State to enable the State to reconcile the funds collected and paid with the respective State Entity. Accurate Disbursement Reports including but not limited to transaction counts, total dollar volumes, and a breakout of the fees shall be submitted by the 15th of each month. Please describe your company’s ability to meet these requirements. Please outline any quality assurance practices in place to ensure the accuracy of Disbursement Reports. Please outline the process in place for Disbursement Report corrections, including time frame for resolution. Please provide examples of detailed Disbursement Report capability.

|  |
| --- |
| NIC Indiana understands and will comply. The proposed solution is currently configured in the State to meet these disbursement requirements and will be configured to individual State Entities, as outlined in each State Entity SOW.  The Payment Platform includes a robust disbursement engine that is designed specifically for government. Settlement of funds starts with establishing the proper hierarchical structure of merchants and services within the platform. There are a variety of configurations that can accommodate each state agency at an agency or specific service level. For instance, there are many cases when an agency prefers or requires disbursing funds for a specific service to a separate bank account in comparison to another unrelated service within the same agency. Likewise, a specific service may require funds collected in a transaction for a specific item to be deposited into a different account than another item on the same order. All of this is made possible through NIC’s disbursement engine capabilities.  Based on the configurations, the NIC Payment Platform will set an effective funding date for each transaction at the time of successful capture. On the configured effective funding date, the system will batch the transactions and create and transmit a NACHA file to the bank for processing and depositing to the Agency accounts. Each day’s settlement reconciliation files can be delivered via SFTP or accessed any time online to support state agency integration into the State’s ERP system and reconciliation activities against bank transactions.  For additional quality control and transparency, the NIC Payment Engine Merchant Disbursement Report displays the disbursements (deposits) made to department bank accounts listed by service. This report allows staff to verify fund transfers have been completed, identify pending transfers, and reconcile treasury bank accounts. Since all data is retained for reporting, there are no limitations to the State’s access to historical data. A copy of transaction-based data stored in the NIC Payment Engine will be retained upon termination of the contract and will be used solely for audit and defensive purposes.    To manage disbursement report corrections, the platform is designed to receive and process settlement files from the third-party processor daily. These settlement files contain details of disputed payments, chargebacks, and disputes settled in the merchant’s favor. These transactions are loaded into the NIC Payment Platform and notification is sent to NIC staff and the State based on a pre-defined workflow preference of the State or individual agencies as directed. This notice is typically leveraged by the State agencies to mark or backout the transaction in the system of record. Upon winning the dispute, a representment is loaded on the order in the Payment Platform and the State is notified of dispute resolution.  NIC Indiana’s detailed service code setup process is in place to mitigate any potential disbursement errors. First, we conduct an end-to-end test and require confirmation of the funds received, to the requested bank account, by the agency/partner. This is required and completed for all new payment processing requests that also includes a new bank account. This will confirm the bank account is set up properly. Additionally, when setting up the new service code in The NIC TPE® Payment Engine, NIC Indiana indicates the correct split of funds to be disbursed to the agency for each transaction. Once setup properly, TPE automatically disburses the expected amount for each transaction. NIC Indiana along with the agency partner test to ensure the right amount is being disbursed to the state before pushing the service to production. TPE has several reports available, including a Merchant Disbursement Report used to verify the disbursed amount matches with the expected amount. This report provides to the agency the exact amount that will be disbursed and should match the agency’s internal reporting from their applications. The Merchant Disbursement Report can be pulled based on the transaction date, the effective date or the disbursement date making reconciliation easier for our agency partners. Access to this system is available for all agencies, as needed. In the event of a discrepancy, NIC Indiana will research it to find the problem and if a resolution is needed, it is completed within one business day. Dependent upon the findings, the disbursement is corrected and disbursed through TPE as expected, or a one-time ACH is sent to the disbursement bank, via NIC, if the TPE disbursement method is not an option.  NIC’s standard reports will allow agencies to complete all of the following tasks plus numerous other activities:   * Error resolution * Customer service/transaction inquiries * Audit trails (by User ID, Batch ID, Transaction ID) * Efficient reconciliation * Daily transaction reporting   Case Study  The NIC Payment Platform distributes up to $30 million in payments to nearly 300 individual Colorado agency accounts daily. And in Idaho, the platform distributes over 450 types of payments to individual accounts daily. Disbursements range from school districts, across multiple city departments, individual county departments, and all state agencies. The standard use case is a single disbursement linked to a single transaction. The NIC Payment Platform creates ACH files to initiate ACH debit and credit transactions as well as submitting daily settlement files to state treasury systems for reconciling payment details. In both Colorado and Idaho, service users have the option of receiving automated daily disbursements reports by email or by connecting to an API in the billing system for pulling the disbursement data into an automated settlement process. |

* + - 1. The Contractor must take responsibility for researching all merchant processor notifications of a chargeback to a customer's credit card account. The Contractor must act on behalf of and in the best interest of the State regarding chargebacks and provide a Chargeback Report to the State. The Contractor must have the ability to notify, via email, on a daily basis, an unlimited number State Entity contacts. Please provide your company’s current process for the research, notification and reporting of chargebacks. Please include an example report.

|  |
| --- |
| In the event of a chargeback, the typical NIC model is that the NIC Indiana team would become the first line of defense for managing representments for the card network requests. NIC Indiana coordinates with the appropriate State Entity personnel to ensure they are successfully resolved. This is a unique model that allows the State to excel at serving its constituents, while allowing NIC Indiana to manage all aspects of the merchant services.  While NIC Indiana will try its best to successfully resolve Chargebacks, there is always a chance we are unable to resolve a dispute. In the event NIC Indiana is not able to resolve the dispute, we will notify the State Entity so that they can mark the customer’s payment as “outstanding” in that department’s system.  As the Merchant of Record, NIC Indiana will receive notification of all customer disputes (chargeback requests). NIC Indiana will notify the State Entity within two (2) business days of the receipt of the transaction but will work directly with the card issuer to provide all the supporting documentation required to successfully fight the dispute.  All credit card chargebacks are captured in the NIC Payment Platform and associated with the original transaction. The administrative site has a specific report allowing the spending units to report on any chargebacks. Under a model where NIC Indiana acts as the Merchant of Record, we will coordinate with the State Entity and be responsible for responding to credit card chargebacks. In the event a chargeback cannot be resolved through correspondence with the issuing bank the State Entity would ultimately be responsible for the return of the principal or statutory fees.  A key benefit of NIC’s payment engine is that it can be configured to handle various flow of funds. Chargebacks can be netted off of future disbursements, invoiced monthly or be debited from a designated bank account. The platform is designed to receive and process settlement files from the third-party processor daily. These settlement files contain details of disputed payments, chargebacks, and disputes settled in the merchant’s favor. These transactions are loaded into the NIC Payment Platform and notification is sent to NIC staff and the State based on a pre-defined workflow preference of the State or individual agencies as directed. This notice is typically leveraged by the State agencies to mark or backout the transaction in the system of record. Upon winning the dispute, a representment is loaded on the order in the Payment Platform and the State is notified of dispute resolution. |

* + - 1. Please outline your company’s current process for researching and approving refunds. Please provide details on your company’s capabilities for refunds to be executed at the State Entity level and any safeguards provided for that process. Respondents must offer the capability to process refunds at both the online or terminal level for all transactions. Please provide details on POS functionality to process refunds at the terminal level utilizing a manager override or password protected process. Please include details on the communication tools utilized to manage the refund process with the State, any reports, and resolution time frames applicable.

|  |
| --- |
| The administrative interface of the platform allows authorized users, including cashiers leveraging POS terminals, to issue full and/or partial refunds of all captured transactions. The authorized user will log into the NIC Payment Platform, search for the order, drill into the payment transaction, and select ‘create refund’. The screen presented next will allow the user to enter 100% or less of the remaining available amount for refund. Amounts available for refund are equal to the total payment captured, less any returns, chargebacks, or partially issued refunds. Refunding can also be accomplished using APIs for automated system-to-system refunds. Role based access to perform refunds can be at the agency, division, and terminal levels to ensure proper separation of duties.  The NIC Payment Platform allows voids through two separate processes. For transactions that are in an authorized state, awaiting a batch capture process, an authorized user can log into the NIC Payment Platform user interface and ‘cancel’ the transaction. This process voids the transaction in the NIC Payment Platform and voids the pending authorization on the account. The funds in this scenario will never be captured.  If a transaction is authorized and captured, an authorized user can log into the Payment Platform user interface and ‘refund’ the transaction. If the refund is completed on the same business day, the transaction will be voided, and the funds will not be settled. Please see the refunding and voiding transactions workflow below:  Refund (Void) Administrative Screen    Refund (Void) Confirmation Screen    The proposed Payment Platform provides the following standard refund reports:   * **Refund Detail** ¾ Shows refunds made for a particular service or set of services. * **Refund Summary** ¾ Shows the volume of refunds processed, the total refund amount, and the amount paid back to the merchant. |

* + - 1. Please describe the current safeguards in place to prevent double-billing, over drawn credit cards, and fraudulent charges. Please provide your company’s ability to meet the following fraud prevention requirements: an AVS feature, requiring the CVV from payers, behavior reports based on criteria defined by State Entity, real-time alerts (State Entity criteria), State Entity-controlled profile blocks (and removals), and State Entity-initiated refund requests to Contractor. Please include details on the different levels of checking your solution offers and the recommended timeframe. Please provide details on your ability to work collaboratively with the State to incorporate unique requirements.

|  |
| --- |
| The NIC Payment Platform has numerous configurable safeguards in place to prevent double-billing, over drawn credit cards, and fraudulent charges.  The Payment Platform includes configurable fraud controls that allow the government partner to require an AVS verification as part of the authorization/capture process. CVV is also a configurable parameter that many government partners prefer to take advantage of. Additionally, the NIC Payment Platform is compliant with the latest NACHA rules requiring real-time account verification when processing an ACH/eCheck. This additional fraud prevention tactic is included at no additional cost to our government partners.  The platform also has duplicate payment controls that allow for configurable protection against duplicate payments being processed. In support of duplicate payment prevention, a hash is created with details of the transaction and that hash is blocked from being repeated or duplicated for a set period. This period can be set as low as a few minutes up to a full day. In addition, if a completely new order is started, the hash would be different as the details of the transactions would differ from the previous order, allowing customers to make similar payments without them being rejected as duplicate payments. This is important to support services that allow more than one same dollar amount transaction, such as a toll system or hunting lottery for example.  With regard to preventing over drawn credit cards, the NIC Payment Platform is configurable to include an authorization/capture process that can complete a credit card transaction in two steps. If enabled, the Payment Platform will perform an authorization on a credit card to verify the funds are available. If the authorization is successful, the integrated agency application can then initiate the backend processes that complete the transaction in their system, then make a capture call to the Payment Platform in order to complete the transaction. This provides added flexibility to the government partner, and often streamlines the checkout process in the partner system.  As with any fraudulent tactic, bad actors continually look for methods to bypass safeguards. The NIC Payment Platform offers configuration that provides our government partners with control to make additional decisions regarding payments processed through their systems. Similar to the platform’s duplicate blocking capabilities, the NIC Payment Platform also has the ability to block customers from leveraging the same payment method in the event of unwanted transaction behavior. The payment platform can either allow for an agency administrator to selectively block and unblock a customer from continuing to leverage a specific payment method for future transactions, as well as establish an automated business rule specific to failed payment attempts. NIC will work with the State to determine which method is preferred and to configure the business rule to adhere to the State’s desired outcome. This may include factors such as how long the block is in place, if it is for a specific service or the state as a whole, and whether a State authority has the ability to remove the payment method from the blocked list.  NIC Indiana has extensive experience with collaborating with our government partners to implementing unique safeguards specific to their business. This may include automated reporting based on specific criteria, or additional controls built into a system. To support this effort NIC Indiana has partnered with Certified Fraud & Forensic Investigation (CFFI), an Indiana CPA and private investigations firm, who specializes in fraud detection and prevention. CFFI has partnered with numerous government partners in the past and provides services such as tax fraud investigations, government monitoring, fraud auditing, and more. NIC’s robust Payment Platform combined with CFFI’s extensive knowledge in the realm of fraud will help to ensure Indiana has effective tactics to reduce and prevent fraud. |

* + - 1. Please describe your company’s internal Quality Assurance (QA) testing, End to End testing and external Customer Acceptance (CA) testing process. Please provide your process and ability to test each phase and requirement of the payment processing lifecycle from initiation to bank settlement.

|  |
| --- |
| NIC Indiana has an established and proven process to ensure high levels of Quality Assurance, validated and approved End to End testing process, as well as standardized Customer Acceptance of the setup, configuration, and disbursement profiles by service.  NIC Indiana will work to setup or update any payment service following a defined and approved process. The following depicts the high-level overview of this process.   * Document requirements as discovered with the customer in the Statement of Work * Customer will review, approve, and sign the SOW prior to work beginning * NIC Indiana will then work to configure the Payment Platform in the TEST system based on the preferences of the agency in the SOW. This includes: * Setup of service code for the associate service utilizing the configurations requested of the agency, including but not limited to: * Amount thresholds * Duplicate blocking preference * AVS and CVV preferences * Disbursement profiles for each state entity receiving funds from each transaction * User interface design configuration * Disbursement rules and configuration of new bank account(s) if required. * New bank account setup entails a separate approval process including a bank letter specifying the account details, internal NIC approvals, and external customer approvals * Internal QA process begins to ensure configuration meets the configurations specified within the SOW. * NIC Indiana uses Jira for internal defect management including: * Test case creation * Test case execution * Issue submission, management, and resolution * Customer Acceptance, commonly referred to as User Acceptance Testing takes place on internal QA is complete and all defects are resolved * Upon completion of UAT approval, configuration is migrated to the PRODUCTION environment. * Internal QA verifies all configuration has been migrated correctly. The system is then ready for final UAT and End to End testing. * End to End testing includes: * For new disbursement accounts, an end-to-end “penny test” will be performed to ensure proper routing to the specified bank. * A series of test transactions that validate all configuration and the final fee and deposits match the configuration in the SOW. * Upon completion of the End-to-End testing, which is completed in coordination with the customer, the customer submits final signature approvals on the SOW and the service is ready for production use. |

* + 1. **Contract Management, Customer Support, and Personnel**
       1. Please describe the account management team structure including names, contact information, and resumes where possible, and services each individual or group will perform.

|  |
| --- |
| NIC Indiana is proud to present a highly skilled account management team to support the requirements of the State. Each team member has had the pleasure of serving the State of Indiana for several years and has extensive knowledge of the various systems across the state. Most importantly, this is a team of Hoosiers located across the street from the downtown State Government campus who will be readily available for support, consultation, and planning the future of payment processing in Indiana.  The primary account management team will be paired with a robust team of MBE, WBE, and IVOSB partners who are experts in their craft and were handpicked for the value they will bring to the payment processing engagement.  NIC Indiana is proud to present the following members of the State of Indiana payment processing account management team and service delivery personnel.  **Core Account Management Team/Service Delivery Personnel**  *Adriana Gao*  *Project Role: Account Manager*  Adriana has worked in the project management field for ten years and counting. She possesses great skills in cross-functional team leadership, business intelligence, business analysis, strategic planning and much more. During Adriana’s tenure with NIC Indiana, she has successfully led upwards of 14-20 simultaneous projects from small to large at any given time. She has provided great leadership within the team as well as identifying and executing changes to help the team work more efficiently. Her background and strong project management skills will be a great fit to lead the Account Management Team as the Account Manager. Please see her resume in the attachment *F.4 Account Management Team Resumes*.  *Robert Short*  *Project Role: Project Manager*  Robert has worked in the technology field for nearly 16 years starting as a developer and then moving into project management for the last 15 years. Throughout his tenure with NIC Indiana, Robert has led countless projects, assisted agencies with specific needs, helped with training, provided customer support to a multitude of agency partners, and continues to stay at the forefront of new project management methodologies and best practices. Robert’s proven ability to handle projects of all sizes with payment processing ensure he is the right fit to be the Project Manager on the Account Management Team. Please see his resume in the attachment *F.4 Account Management Team Resumes*.  *Joseph (Joe) Mount*  *Project Role: Technical Lead Architect*  Joe started his career as a software consultant ten years ago while studying to earn his Bachelor of Science in Computer Science Degree from Ball State University. Joe brings a great deal of experience in C# programming, T-SQL database administration, web development using .Net Core, ASP.net and REST APIs. In his nearly seven years of experience with NIC Indiana, Joe has become a vital team member in migrating existing applications to the NIC Payment Platform and as a consultant to third parties integrating with the NIC Payment Platform. Joe’s ability to provide top notch support to internal personnel and agency partners, programming skills, and his vast knowledge of NIC Indiana’s payment processing systems makes him the right fit as the Technical Lead Architect on the Account Management Team. Please see his resume in the attachment *F.4 Account Management Team Resumes*.  *Partner Resource*  *Project Role: Technical Lead*  In anticipation of the MuleSoft product being utilized in the technical implementation during the transition period, NIC Indiana will be leveraging the experience of our partner, STLogics, to provide a technical lead with applicable knowledge in MuleSoft. The resource will be identified once a clear understanding of the goals for MuleSoft are identified. This is to ensure the resource as knowledge in relation to the requirements defined during the transition period.  *Garry Chatman*  *Project Role: Customer Service Representative*  Garry has been a strong Customer Service Representative with NIC Indiana for over 13 years. He possesses a natural ability to communicate with our citizen customers, and he will see any problems through to the end. Additionally, through listening to our customers he has identified enhancements to improve the user experience of NIC Indiana’s applications & services. Garry has a great deal of experience and knowledge with NIC Indiana’s payment processing solutions from completing the payment, sending copies of receipts to customers, communicating refund requests to the agency partners, and taking the lead on chargeback requests. His strong communication skills, vast knowledge of NIC Indiana’s payment processing systems and customer service skills make him the perfect fit to be the Customer Service Representative on the Account Management Team. Please see his resume in the attachment *F.4 Account Management Team Resumes*.  *Rodney Caudle*  *Project Role: Qualified Security Auditor*  Rodney brings over 21 years of experience within in the security auditing profession to the Account Management Team. Rodney is a CISSP and leads the penetration testing, incident response and threat intelligence teams for NIC. He provides the security policy and practice leadership for the NIC Payment Platform and supports NIC’s projects across the country. Rodney’s strength and expertise in security auditing will bring a high-level of support to the Account Management Team/Service Delivery Personnel. Please see his resume in the attachment *F.4 Account Management Team Resumes*.  **WBE/MBE/IVOSB Partners**  In addition to the skilled NIC Indiana staff hand-picked to complete the main Account Management Team, NIC Indiana has partnered with several Indiana companies to add additional value to payment services offered under the payment processing request for proposal.  *CFFI, Auditors & Fraud Investigation*  Our Women’s Business Enterprise Subcontractor Partner, Certified Fraud & Forensic Investigations (CFF), will bring their auditing expertise to the Account Management Team. The collective experience includes managing, planning, and performing government audits in accordance with GAGAS standards. They lead and provide guidance for State and Local Government Tax Agencies with regards to developing and monitoring overall tax refund fraud solution with a special emphasis on identifying organized crime groups committing Stolen Identity Refund Fraud (SIRF), building internal business rules to stop and deter bad actors and implementing best practices. Additionally, they bring extensive experience with fraud investigations. Their backgrounds and expertise will bring a great fit to the overall contract for the state.  *aFit Staffing, Inc., Marketing, Project Management & more*  Our Women’s Business Enterprise Subcontractor Partner, aFit Staffing, Inc., will bring a great deal of experience with project management activities, business analysis and marketing to the overall success of this engagement. aFit Staffing has over 27 years of experience with system implementation, maintenance, and operations, as well as over 16 years of experience in State Government specializing in vendor performance management. aFit Staffing is a proven business that will assist the core Account Management Team to provide the best service to the State of Indiana. Their experience with marketing will also be a positive addition to the payment processing services ensuring the continuous secure payment processing growth occurring within the state is properly advertised.  *D&R Freight, LLP, Administrative Back Office Services*  Our Minority Business Enterprise Subcontractor Partner, D&R Freight, LLP, will bring a great deal of experience with administrative back-office services such as tracking equipment utilization, efficiency analysis, product management and much more. D&R Freight’s experience is a perfect fit to track and maintain point of sale equipment inventory, shipping and receiving, and assist the core Account Management Team with other administrative tasks, as needed, to ensure the success of payment processing migrations and continued support after the migration.  *All Things Data, MuleSoft Implementation, Data Reporting & more*  Our Indiana Veteran Owned Small Business Enterprise (IVOSB) Subcontractor Partner, All Things Data, will bring extensive experience with MuleSoft Implementation, Technical Consulting Services, Data Reporting and providing technical resources as needed.  *STLogics, MuleSoft Implementation, IT Consulting Services & more*  Our Minority Business Enterprise Subcontractor Partner, Sahasra Technologies Corp dba STLogics, brings specialized experience with MuleSoft Implementations, Data Analysis, Information Technology Consultation Services, and technical resources as needed to support the state’s desire for MuleSoft integration with the state’s systems. STLogics’ RadCube team will also provide other technical support and resources as needed to assist the Account Management Team’s objectives.  Leveraging the key account management members and partners above, NIC Indiana will scale the team as needed to ensure a successful engagement with the state. The size of the project team will be dependent on the overall quantity of payment engagements and the associated revenues; however, key roles specified within the RFP will be filled as requested. The following organizational chart depicts the suggested project team for the Indiana payment processing opportunity assuming a majority of payment processing engagements are operating under NIC Indiana. |

* + - 1. Describe in detail the controls in place (or proposed) to ensure that your company is providing quality products and services. Explain the method of performance monitoring used and the format this information will be communicated to the State. Describe in detail any quality programs the respondent has implemented, how the benefits are measured, and the results of any programs.

|  |
| --- |
| Project Controls  To ensure NIC Indiana provides secure, reliable, high-quality products and services, our account management team dedicated to the resulting payments contract, will follow well-documented and industry-accepted project management methodologies that leverage specialized tools tailored to meet the SDLC of the projects. To this end, NIC Indiana utilizes both waterfall and agile methodologies within its environment. Each of these methodologies has proven specific benefits to the IN.gov Program, align with needs of the State, while relying on modern development techniques to develop high-quality products.  The selection of one method over another is dependent on the project itself. The characteristics of a project are thoroughly evaluated, and a final determination of project approach is decided. However, all projects completed by NIC Indiana appear as waterfall at the surface. This is due to the contractual requirements of the State, which include definitive deadlines and projects costs.  The ability to be nimble to the rapidly evolving software development industry has allowed NIC Indiana to continue to be a relevant partner to Indiana. The methodologies used, roles leveraged, and structure of the team has been shaped by the 25+ years of working in partnership with the State of Indiana and our 48 employees who are dedicated to the Indiana digital government program.  Performance Monitoring  The NIC Team tracks a wide range of performance indicators and customizes both the metrics collected, as well as the presentation format based on the needs of our agency partners. We frequently provide online dashboards that can be viewed on-demand, as well as longer-form soft copy and hard copy reports. NIC is able to provide daily and weekly digest emails that can be sent to pre-determined distribution lists and include high-visibility metrics like mobile payments or transaction volume. Examples of performance indicators that we typically report include:   * Operational headlines and highlights * Status of projects and change requests in development * New services and enhancements delivered * Transaction counts * Statutory fees collected and disbursed * Customer service and service desk activity by channel * Customer satisfaction survey results * SLA tracking * Security dynamics   NIC leverages a web-based notification solution to communicate service degradation to both the NIC team and our government partners. This solution supports notifications via Email, Text Messaging, RSS Feeds, and a website. As standard practice, the NIC support team makes first communication moments after we declare a Severity 1 incident and then every 30 minutes until resolution. There are variable configurations available, so NIC will work with the state to determine the appropriate alerts for state staff, and the final communication plan for notifications of system outages or degradation.  Quality Program Implemented  NIC’s approach to implementing the payment platform at the State Entity level is a process forged through many implementations for government agencies across the country. In our best practice, NIC works with our state government partners to design a simplified merchant services architecture that consolidates merchant accounts and merchant processors. The effort will reduce complexity and costs, create a more manageable solution, and simplify new merchant onboarding.  Once the initial hierarchy and foundation are established, NIC uses a standard approach for onboarding each agency and service. This process includes discovery with the agency and appropriate stakeholders to understand the payment processing options that will be required. This discovery process drives additional provisioning workflows, such as merchant boarding activities, sub-merchant agreements, American Express boarding, ACH setup, etc.  On a per service basis the NIC Account Management team will also configure NIC payment platform setup and configurations. This includes financial testing workflow, where an end-to-end “penny test” will be performed for each settlement account NIC adds to the platform. Once financial testing has occurred for an account, other services can leverage this account for settlement, streamlining on-going integration of services that make use of the account.  Once the foundational elements are in place, then the process of acquiring new merchant IDs can be obtained within 10-21 calendar days. Most new payment methods, such as a state entity expanding from credit card and debit cards to now include ACH is a simple configuration change on the platform. This rapid timeline is also the case when adding a new service under an existing agency participant hierarchy on the platform. As a nod towards efficiency, the NIC Payment Platform supports the use of soft descriptors to allow for the same merchant ID to be leveraged for certain eCommerce implementations, cutting out the time for new merchant ID issuance in many cases. |

* + - 1. Please provide, in detail, your company’s current issue resolution and escalation plan. Please include details on the approval process to change, update or modify the resolution and escalation processes. Please include an example of the tracking system utilized and the reporting generated.

|  |
| --- |
| NIC Indiana leverages vFire VSM, the tool leveraged by the Indiana Office of Technology, for the reporting and communication of issues and their resolutions.  NIC Indiana leverages a Queue Manager (project manager) to oversee the issue resolutions process. The role of the Queue Manager is to triage the tickets that are received for production systems. As issues are reported, the Queue Manager receives and assesses the information submitted to determine if it is an issue, or if it is a request to enhance the application. Once validated as an issue, a ticket is created in Jira, utilized internally at NIC Indiana, which is then assigned to the development team for resolution. Enhancements follow a separate change management process approved by the State. The Queue Manager communicates to the customer through vFire VSM indicating the ticket was received, communicates with the internal teams to determine status, and provides regular updates to the customer at specified time intervals determined by the issue type. In this role, the Queue Manager serves as the liaison between the internal team and the agency for all communications. Additionally, the Queue Manager ensures all reported items remain in compliance with the service level agreement in place.  Upon diagnosis and proposed resolution path, NIC Indiana completes the fix in the QA environment for internal testing and approval. Upon validation of resolution in QA, deployment to the UAT environment is coordinated with the agency. NIC Indiana works closely with the agency partner to ensure the proper fix was put in place. Once UAT approval is received by the agency, all parties coordinate a deployment to production. In the event an issue affects more than one agency partner, NIC Indiana follows the State’s approved CMR process to ensure all impacted agencies have an opportunity to test, validate, and approve the scheduled day and time for deployment. In most cases, CMR requests are deployed Sunday mornings between 6am and 10am; however, there is an approved escalation process to implement changes more quickly when necessary.  The streamlined flow, dedicated resources, and continuous monitoring of these submissions allows NIC Indiana to triage and rectify issues or bugs submitted by its customers quickly and efficiently.  Additionally, NIC Indiana leverages vFire for customer support request such as billing inquiries, refunds, or other tasks. An example of a refund ticket received via vFire is included below.    A major benefit of vFire is that the product tracts time to resolution to ensure all requests are completed within the specified SLA. The state is able to pull a report at any time to review a list of items submitted as well as the time it took to resolve. In many cases, SLA escalation emails are automatically sent to IOT and NIC staff in the event a ticket is nearing, or surpassed, the SLA threshold. The following image depicts a real-time search of tickets within vFire.    Changes, updates or modifications to the program’s resolution and escalation processes are presented to and reviewed by the senior management team for NIC Indiana and the Payment Oversight Committee at NIC, if appropriate, and communicated with the State for approval prior to implementation. |

* + - 1. Please provide a detailed description of your company’s customer support team, staffing, hours of operation, offerings, and procedures. Please provide details on any customer support services your company offers that are not currently contemplated in the scope of this RFP.

|  |
| --- |
| NIC Indiana can handle English and Spanish and currently supports multiple channels of customer support for the payment solution. For the majority of services, the help desk team is available Monday - Friday from 8am - 5pm EST. This team is accessible by toll-free number, email, or fax. There is also a monitored voicemail if a caller chooses to leave a message for a return call at a later time. NIC Indiana has staff available, on-call, 24 hours a day, 7 days a week, 365 days a year for the State Entity to contact in the case of a payment processing emergency.  For systems requiring a higher level of service, a third-party call center partner is utilized. The call center is able to provide human operator support with the ability to do Integrated Voice Response. In the past, we have leveraged this team for Indiana on short notice and provide separate temporary toll-free numbers if warranted. This solution is able to support peak usage times, one-off capacity increases, and future call center needs (voice sales, fulfillment, etc.).  In addition to these services, support request forms have been integrated into various services and applications and are a critical aspect of the support workflow and escalation process. Some of these forms notify NIC Indiana staff 24x7x365 depending on the critical nature of the submission type. |

* + - 1. Please describe your company’s current policy on personnel background checks, including frequency and types conducted. Please confirm your ability to meet all requirements outlined in Attachment J- Scope of Work, Section 1.4.3.1(2)(v)(1).

|  |
| --- |
| NIC Indiana has read, understands, currently complies, and will comply in the future with the *(1) Background Checks* requirements in *Attachment J - Scope of Work*. Additionally, NIC has a detailed code of conduct policy, which is continuously improved and expanded to ensure the integrity of NIC, our clients, our employees, and the public assets we are entrusted with. NIC takes the following measure to ensure compliance with NIC code of business conduct:   * All NIC employees are required to undergo and pass a pre-employment background check. * Within the first 30 days of employment, employees are required to participate in new employee training conducted by NIC, which covers company policies as it pertains to Security, Code of Business Conduct and Ethics. * All employees are required to undertake annual Code of Conduct and Reporting Hotline training * NIC has an anonymous hotline for employees to report workplace fraud or theft, and other potential violations as it pertains to NIC’s Code of Business Conduct and Ethics. |

* + 1. **Reporting**
       1. Please describe your company’s online reporting system including details regarding accessibility to State users and the features and functionalities available. This system shall be an aggregation of all State entity platforms and provide a single point of access to records across all State Entity users. Please describe your company’s ability to provide enterprise reporting across all State associated merchant account for transactions, refunds, & charge backs.

|  |
| --- |
| One of the key distinguishing factors of the NIC Payment Platform is the ability to create hierarchy reporting for each agency, department, or jurisdiction for all payment types, and also aggregate those reports. NIC Indiana provides access to the NIC Payment Platform’s administrative interface, which is controlled at the user level, agency level, and service level, ensuring users only have access to information for which they have been granted privileges as assigned by an administrator of the platform. The platform’s merchant setup is hierarchical allowing the State to provide role-based security for each participating agency. Agency staff is granted access to support refund and void capabilities, as well as financial reporting and research tools based on their defined role within the hierarchy. Enterprise Managers are given access at the highest level to view reports for the entire program. This hierarchy allows NIC to define the structure to have the concepts of State Agencies or entities and Services, which could be representative of a separation by merchant number. This hierarchical system will give a state agency’s central office access to view and report on individual merchant IDs for any office or division or at a consolidated level across a division or the entire department. In addition, reports can be scheduled on a per agency or service basis, so they are sent to the appropriate State admins instead of having to manually retrieve them.  Within the NIC Payment Platform, payment processing data is made available via a wide variety of reporting features. Reports range from summary reports to detail reports showing line-item level data. The NIC Payment Platform, already implemented in the State, provides the flexibility to meet all of the State’s reporting requirements defined in this RFP, including out-of-the box and ad hoc capabilities to provide granular transaction and data exchange reports that meet accessibility, configurability, search output formats, transmission frequency, sorting, and level of detail desired.  NIC provides real-time online reconciliation reports to authorized staff through our secure web-based reporting interface. These reports can be filtered in a multitude of ways including but not limited to custom date range, location, and payment type.  This information can also be used to create reports that match deposits to statements, match return and refund information to settlements and reconcile batches. Not only does this process save time in reconciliation but improves the efficiency of recording journal entries for the different services. The solution provides the ability to reconcile bank activity to each deposit daily.  The following list represents a sample of the standard reports in the NIC Payment Platform:   * **Invoice Detail**: Shows the order and invoice dates, invoice amounts, merchant and processor COS, and total profit by Order ID. * **Invoice Item Detail**: Shows the dollar and volume of items invoiced by merchant/service and SKU. * **Invoice Item Summary**: Shows the sum of dollar and volume of items invoiced by merchant/service and SKU. * **Invoice Summary**: Shows the volume of invoices generated, invoice amounts, merchant cost of sales (COS), and total profit (or loss). * **Merchant Disbursements**: Shows disbursements made to merchants listed by service. * **Net Revenue**: Shows the total revenue, merchant COS, and net profit for a selected merchant/service, as well as the total volume of invoices, refunds, and returns processed. * **Order Detail**: Detail of orders including reference ID, payment type, invoice amounts, merchant and processor COS and total profit. * **Order Item Summary**: Shows the sum of dollar and volume of items ordered by merchant/service and SKU. * **Order Summary**: Shows the volume of orders generated, order amounts, invoice amounts, and total profit. * **Refund Detail**: Shows refunds made for a particular service or set of services. * **Refund Summary**: Shows the volume of refunds processed, the total refund amount, and the amount paid back to the merchant. * **Returns Detail**: Shows returns made for a particular service or set of services. * **Returns Summary**: Shows the volume of returns, the total return amount, and the amount the merchant paid back. |

* + - 1. Please confirm your ability to provide same day and ad-hoc reporting. Please provide your company’s capabilities to provide daily reconciliation reporting at the terminal level. Please provide details surrounding your capability to provide customizable field level details by State Entity user for reconciliation reporting. Please provide your ability to provide custom reports, such as Social Security number frequency, and the time frame required to create and provide custom reports. Please provide examples that align with the requested reports in Attachment J-Scope of Work, Section 1.4.3 (3). Please include descriptions and examples of any additional, applicable reports your company can provide. Please include supporting details and examples for the following reporting requirements: 1- Reports shall have the ability to show aggregated details for the entire requested time period or individual details for each date requested. 2- Reports shall have the ability to include data for all transactions throughout the life of the contract. 3- Reports shall be available at the transaction by terminal detail level. Please describe the functionality available for the searching, saving, extracting and printing. All reporting features and functionalities are to be provided at no cost to the State.

|  |
| --- |
| NIC Indiana can provide same day and ad hoc reporting utilizing the NIC Payment Platform administrative site’s reporting capabilities. This system is in use today in Indiana under our current contract providing the services requested by the RFP, and state staff are familiar with using this system to support their reporting and transaction management needs.  One of the key distinguishing factors of the NIC Payment Platform is the ability to create hierarchy reporting for each agency, department, or jurisdiction for all payment types. Within the NIC Payment Platform, all payment processing data is made available via a wide variety of reporting features. Reports range from summary reports to detail reports showing line-item level data. Reports can be run directly from the administration site as needed or be scheduled to be run and then delivered securely to the recipient either through an SFTP server or through an email delivery.  The platform’s standard reports will allow for State Entities to complete all of the following tasks plus numerous other activities:   * Error resolution * Customer service/transaction inquiries * Audit trails (by User ID, Batch ID, Transaction ID) * Efficient reconciliation * Daily transaction reporting   Additionally, reports can be exported in XML, PDF, MHTML, Excel, TIFF, Word, CSV, CSV-Data Only, GL Service, CSV Text, and Pipe Delimited format.  Ad-Hoc Reporting  The NIC Payment Platform includes out-of-the box and ad hoc capabilities to provide granular transaction and data exchange reports that meet the accessibility, configurability, search output formats, transmission frequency, sorting, and level of detail specified in the RFP.  NIC will work with State Entities to define scheduled and on-demand, same-day ad hoc reporting that meets the needs of the State and specific agencies, including a procedure to request new reports. The NIC Payment Platform provides both real-time customer service/administration and transaction financial reporting for agency personnel managing accounting and payment reconciliation.  The advanced Search page allows the user to search with standard options, by customer, credit card, bank account information, billing, order properties, and date range and get a report back for that criteria.  Please see a screen shot of the Advanced Search functionality below:    Daily Reconciliation Reporting  NIC provides real-time online reconciliation reports to authorized staff through our secure web-based reporting interface. The NIC Payment Platform does not restrict access to reporting against historical data, allowing agencies to run analysis against data from the beginning of the contract to the current date. Leveraging NIC’s Net Revenue and Invoice Detail reports, the agency can perform financial analysis on fees and transactions processed for the period. Additionally, the Net Revenue Details report allows the user to perform analysis by card and payment type for review of processing trends and fee analysis. All of these reports can be delivered on a schedule or run ad hoc and exported in a variety of exportable formats. These reports can be filtered in a multitude of ways including but not limited to custom date range, location, and payment type.  This information can also be used to create reports that match deposits to statements, match return and refund information to settlements and reconcile batches. Not only does this process save time in reconciliation but improves the efficiency of recording journal entries for the different services. The solution provides the ability to reconcile bank activity to each deposit daily.  Custom Reports  The NIC Payment Platform provides the ability to create custom ad hoc reports based on the transaction and user data as described above. In addition, the calling application can pass order or line-item attributes to store as metadata they want to associate with the payment transaction. These attributes can then be exported and leveraged in a custom report designed to the specifications requested by the agency. Additionally, the attributes can be extracted by our government partners at any time using existing out-of-the-box exporting features.  It is rare that the ad hoc advanced search does not provide the data needed to our state partners, however in that case, the NIC Indiana team can develop custom reports for agencies based for instances where there needs to be some actions performed on the data to get the information for the report. The timeline for these reports is variable based on the scope of the request, but typically custom report requests can be completed within a week if there is not a high volume of requests.  Report Examples  Some example reports follow.  Transaction Volume & Dollars Processed, Summarized by Payment Type Report    Merchant Disbursement Report    Invoice Detail Report    Order Item Detail Report      In addition to the standard out of the box reporting, NIC Indiana is able to provide dashboards highlighting key metrics is a roll-up and drill-down methodology. Payment processing dashboards are provided today and include detailed information. Additionally, NIC Indiana is currently working with AWS to implement QuickSight reporting within the state. Upon completion, dashboards such as the below will be available to our government partners. This will provide real-time data to analyze payment processing activity and trends, |

* + - 1. Please describe the process and timeframe to set up users and the ability to restrict access based on the criteria provided in Attachment J- Scope of Work Section 1.4.3.1.3. Please provide details on the training, including examples of user guides, provided by your company to all users accessing the reporting system. Please outline the process and frequency of training and what on demand resources are available to assist State users.

|  |
| --- |
| User Access  NIC provides access to the NIC Payment Platform’s administrative interface, which is controlled at the user level, agency level and service level, ensuring users only have access to information for which they have been granted privileges as assigned by an administrator of the platform. To request administrative user accounts, an authorized agency representative will submit a request to NIC Indiana’s Finance Administrator with the list of users needing access to the NIC Payment Platform’s TPE® administrative site. Requests for new user accounts will be vetted, approved, and fulfilled typically within 1-2 business days of being requested. Temporary credentials will be transmitted directly to the new user’s email with instructions on how to sign in and finalize the setup of their account.  The platform’s merchant setup is hierarchical allowing the State to provide role-based security for each participating agency. Agency staff is granted access to support refund and void capabilities, as well as financial reporting and research tools based on their defined role within the hierarchy. Enterprise Managers are given access at the highest level to view reports for the entire program. This hierarchy allows NIC to define the structure to have the concepts of State Agencies or entities and Services, which could be representative of a separation by merchant number. This hierarchical system will give a state agency’s central office access to view and report on individual merchant IDs for any office or division or at a consolidated level across a division or the entire department. In addition, reports can be scheduled on a per agency or service basis, so they are sent to the appropriate State admins instead of having to retrieve them.  NIC corporate security policy requires all accounts to have an owner assigned to them. Account managers are responsible for requesting permissions and access for the accounts necessary to perform business functions. Modifications of group memberships and account permissions are performed in accordance with NIC Corporate Security policy. Approval from management and security operations is required for all account creation and modifications. NIC corporate security policy requires access be granted based on least privileges needed to accomplish the business functions assigned and requires separation of duties between developers of applications and administrators of production environments.  Account usage is monitored through central log consolidation to a SIEM tool for analysis and alerting by the security operations team. User Behavior Analytics (UBA) approaches are used to analyze the data in the SIEM tool to identify patterns of traffic caused by user behaviors, both normal and malicious.  Training  Training government staff on the NIC Payment Platform is a critical part of providing exceptional services to Indiana. Upon Secondary SOW awards, NIC will conduct kick-off meetings with key project sponsors to determine the appropriate implementation and training schedules. Regularly scheduled, web-based, technical, and security training sessions for staff and administrators for the NIC Payment Platform will also be provided.  As part of the overall transition, NIC Indiana will establish training plans for state staff and technical resources to provide an overview of the NIC Payment Platform:   * Identifying and cataloging all applications requiring payment services * Identifying all integration points * Understanding financial reports, flow of funds, and reconciliation * Handling chargebacks, refunds, returns, and any other exceptions * PCI Do’s and Don’ts * Conducting integration testing * Prioritizing services and determining transition timelines * Post-implementation support processes   NIC Indiana will also schedule follow-up calls with technical resources to share Payment Platform technical integration documentation and will perform follow-up training on NIC’s TPE® Payment Engine reporting and administrative interface. This training is typically done via web conferencing and can include multiple agencies.  NIC Indiana is committed to a true partnership and will provide additional training at any time after implementation, as needed. Phone support, email support, and user guides will be provided to the State.  As an example of training material, NIC has included a copy of its NIC-confidential and proprietary *F.2 CONFIDENTIAL CCP User Guide*. This reference material is an example of the technical documentation provided with training. |

* + 1. **System Upgrades and Maintenance**
       1. Please provide details on the current process for system upgrades and maintenance. Please include details on frequency, communications, advanced notification, time frames. Please provide details on your company’s ability to provide at minimum 2 weeks advance notice of scheduled upgrades and maintenance.

|  |
| --- |
| The PCI Level 1 compliant NIC Payment Platform can accept and processes payments 24 hours a day, 7 days a week. We do this currently on behalf of our government partners nationwide, so every day is a Processing Day. All routine network and server maintenance are completed using Zero Downtime Deployment techniques to ensure that the system remains available for processing during upgrades and other maintenance activities.  A Zero Downtime Deployment is defined as a deployment mechanism which leverages the distributed capabilities and high-availability architecture of a system to gradually deploy upgrades and other changes to the system, in a very controlled and coordinated manner, without impacting the overall availability of the system. Following this approach, each node of a cluster is individually removed from service and then upgraded. Post deployment testing and validation is then conducted on the upgraded node. If successful, the upgraded node is returned to service. This basic process is then repeated until all cluster nodes have been upgraded, validated, and returned to service.  While we do not expect any downtime during the maintenance window, should one be needed, NIC Indiana will notify the State and all impacted agencies of the planned outage and the details of the expected outage at least two weeks prior to the scheduled window if there is a planned outage.  In addition, customers attempting to make a payment will receive an agreed upon error notification on their attempt saying that the system is down currently and for them to try again later with any additional instructions determined in the communication plan. |

* + 1. **Implementation**
       1. Describe in detail your company's proposed Implementation Plan, including tasks to be executed, target dates for completion, identified risks to the project, and any assumptions made for accomplishing the plan. Respondent must describe in detail how it will transition application payment processing integrations to a new processor. Please provide any examples of the respondent's experience with payment processing environments that are as diverse as the State of Indiana’s. Describe the respondent's anticipated level of effort to accomplish this transition. Where the information provided is insufficient, please list any general assumptions that the respondent is making in responding to this inquiry. Please demonstrate the ability to implement the entire Scope of Work, inclusive of all State Entity platforms outlined on Attachment K- State Entity User Requirements and any additional State Entities wishing to on board during the implementation period no later than October 20, 2022.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NIC Indiana is no stranger to implementation plans as part of a statewide engagements. Our largest customer base is State government enterprise engagements, and therefore, NIC has decades of experience across dozens of partners.  As the current provider of approximately 50% of the customers listed in this solicitation, the implementation plan focuses on those service not provided by NIC Indiana today. The implementation approach will classify each payment processing engagement as Standard or Robust. Two focused project groups will be formed to manage each classification. This will allow NIC Indiana to strategically place team resources across the two teams to ensure experts in their field are focused on engagements that complement their skills. Regardless of the classification, each service transitioned to NIC Indiana will follow a standardized and proven process. NIC Indiana has managed thousands of projects through its relationship with the state of Indiana including all of the payment customers we support today, and therefore we are confident our implementation approach will align with the needs of each state agency seamlessly. The high-level tasks and responsible parties can be found in the table below.   |  |  | | --- | --- | | Task | Responsible Parties | | Initiation - Requirements/Process Mapping |  | | Execute Project Kickoff Meeting | NIC Indiana | | Draft Project Charter document | NIC Indiana | | Complete Project Plan with Major Milestones | NIC Indiana | | Review Project Charter document | State Entity | | Complete/Sign-off Project Charter document | NIC Indiana/State Entity/IOT | | Execute Discover Meetings with State Entity | NIC Indiana | | Execute Requirements Meeting(s) |  | | Identify Project Stakeholders | State Entity | | Draft Agenda and Plan Meeting Strategy | NIC Indiana | | Execute Meeting(s) | NIC Indiana | | Draft and Deliver Meeting Minutes | NIC Indiana | | Draft Requirements (including device needs) | NIC Indiana | | Review/Finalize Requirements | State Entity/NIC Indiana | | Approve Requirements | State Entity | | Merchant/Service Code Setup |  | | Provide banking information | State Entity | | Create new service code | NIC Indiana | | Complete End to End Testing | NIC Indiana/State Entity | | Device Procurement (if applicable) |  | | Order the desired quantity of devices | NIC Indiana | | Test and confirm the devices work as expected | NIC Indiana | | Deliver & configure the devices | NIC Indiana/State Entity | | Development & Configuration |  | | Define and Plan Sprint(s) | NIC Indiana | | Execute Sprint | NIC Indiana | | Perform Retrospective | NIC Indiana | | Plan Next Sprint (if applicable) | NIC Indiana | | Data Conversion (if applicable) |  | | Provide data details | State Entity | | Data Analysis | NIC Indiana | | Complete Data Conversion | NIC Indiana/IOT | | Testing |  | | Execute QA | NIC Indiana | | Execute UAT | State Entity | | Execute Security Testing | NIC Indiana | | Resolve Testing Outcomes | NIC Indiana | | Training |  | | Outline Training Plan | NIC Indiana | | Training Documentation | NIC Indiana | | Conduct/Attend Training | NIC Indiana/State Entity | | OCM & Communication |  | | Determine Communication Message/Plan | NIC Indiana/State Entity | | Execute Communication Plan | NIC Indiana/State Entity | | Deployment/Production Stabilization |  | | Draft Deployment Plan Document | NIC Indiana | | Complete Production Cutover Plan document | NIC Indiana | | Document Signatures | NIC Indiana/State Entity/IOT | | Execute tasks from Production Cutover Plan document | NIC Indiana | | Go Live | NIC Indiana | | Test & Verify Deployment is Successful | NIC Indiana/State Entity | | Execute Project Retrospective | NIC Indiana | | Production Stabilization |  | | Continue Post Launch Quality Assurance Testing | NIC Indiana | | Monitor Application Logs | NIC Indiana |   The transition teams at NIC Indiana will be focused on Standard and Robust project classifications as mentioned above. Standard transition will include payment processing engagements wherein the agency application, or process, is utilizing the out-of-the-box product library offered by NIC Indiana with minimal customizations, reporting needs, etc. This accounts for the majority of the projects. The second classification, Robust, includes large-scale payment processing engagements wherein customizations, unique needs, multi-system integration, or other features not leveraged in Standard engagements. NIC has initially identified Department of Child Services, DNR Parks/Campgrounds, Indianapolis Airport, and the Secretary of State INBiz platform along with its participating agencies, Department of Revenue, Department of Workforce Development, and the Professional Licensing Agency, as agencies fitting the Robust category. If it is determined that the integration is less robust than initially estimated upon examination of the detailed requirements, NIC Indiana will adjust the timeline accordingly.  NIC Indiana has based its classifications within Attachment K on its understanding of the scope of each engagement and used the following assumptions.   * **Base:** Those items that can be delivered as part of a base installation without any configuration or customization. * New services NIC Indiana brings onto its platform will require basic configuration. At minimum items such as fee structure, disbursement configuration, and agency preferences will be necessary to begin accepting payments. This will be the case for any provider. Therefore, NIC Indiana indicated all its existing services provided to the state were ‘Base’, and those not currently offered by NIC Indiana were ‘Configuration’. All services presented in Attachment K are specified by NIC as either Base or Configuration and are supported. * **Low, Medium, High:** NIC Indiana assumed that the hours specified in ‘Low’, ‘Medium’, and ‘High’ were related to the work performed by NIC Indiana. NIC Indiana is not familiar with the details of agency systems that it is not responsible for and cannot speak for the time required by the agency or its third-party provider. That being said, NIC offers detailed integration guides and will provide assistance as needed to help with integration to our products. In scenarios where NIC Indiana provides an off-the-shelf product to replace the scope of the system, NIC Indiana will provide the product with no technical effort required by the agency.   Using the details above, please see attached file *F.7 Implementation Project Schedule* for details pertaining to the dates associated with the transition. Projects were listed in order based on NIC Indiana’s understanding of peak timeframes for individual agencies. We understand that the order of the projects and timelines are subject to change after working with the State through the SOW process, and NIC’s nimble team will be ready and able to pivot as needed.  The primary risk identified with the transition will be availability of agency third-party vendors responsible for the systems as well as agency technical resources if developed/maintained in-house. NIC understands that each agency may have other high priority initiatives in progress and will work collaboratively with the agencies to ensure the dates selected for transition are as convenient as possible to help ensure success for both parties.  NIC Indiana is assuming that, in most cases, existing agency systems will be leveraged for business functions, or that the agency will leverage one of NIC Indiana’s low-code no-code products to reduce the amount of custom development that must be completed during the 12-month transition. That said, NIC Indiana will work with the state to identify, as early as possible, any systems that will need to be rebuilt. Application development is another service offering from NIC Indiana, with more than 176 services in production on behalf of our Indiana government partners.  The NIC Payment Platform is built to be integrated into third-party products, to be used as standalone system, or both. NIC Indiana will leverage these products as mentioned throughout this proposal. NIC will consult with each agency to determine which product will best serve the agency. This list of products is as follows and will expand as NIC continues to invest in its Payment Platform.   * AppEngine for low-code no-code online form creation and management * Over-the-Counter (OTC) module for Point of Sale transactions * Common Checkout Pages (CCP) module for customized online web payment pages * Customer Database (CDB) module for billing and recurring payments * Prompt Pay module for SMS and email-based payments for citizens * OnTheGo® Pay module for taking POS credit and debit card payments on a mobile device in the field * Gov2Go® Pay digital wallet that streamlines government payments * Fiserv CheckFreePay integration offers the ability to accept cash through Fiserv’s CheckFreePay agent network   NIC Indiana is confident that it will be able to successfully provide a product or service to replace each of the solutions in production today.  In order to describe the anticipated level of effort to accomplish this transition, NIC Indiana will use the assumption that all services NIC does not offer today will be migrating to NIC during the transition period. With this assumption, NIC Indiana anticipates it will take 12 months to migrate all services to NIC Indiana. This will be accomplished with a team of 15 individuals and the support of the 5 MBW/WBE/IVOSB partners that have been handpicked to provide tremendous value to the project and the state. Please see the attached file *F.8 Implementation Project Plan* for a detailed plan outlining the work necessary to accomplish this task and *F.7 Implementation Project Schedule* for the detailed project schedule/timeline.  As a current payment provider to the state, NIC Indiana delivers digital government services to more than 176 Indiana agency partners including local, state, and quasi-governmental agencies. Through nearly 300 years of combined knowledge focused solely on Indiana, the NIC Indiana staff are experts in the government space and have solid relationships with nearly all government entities in the state. NIC Indiana’s parent company, NIC, manages business-to-government and citizen-to-government applications on behalf of more than half the states in the U.S., including several statewide payment processing engagements.  Serving thousands of quasi, local, state, and federal accounts, NIC’s products and services are built on the needs of government, resulting in NIC being the largest payment processor solely focused on delivery of digital government services. NIC’s expertise surpasses that of just payment processing for our partners. In most engagements NIC is responsible for the full development lifecycle of electronic government services which allows NIC staff to be highly educated on the innerworkings of a vast variety of government agencies and their processes.  All told, NIC provides comprehensive payment processing services at the state and local and quasi-governmental level in 32 states, as well as payment services for projects on behalf of 15 federal agencies including Recreation.gov. |

* + - 1. As part of the Contractor’s response, an initial Implementation State Entity Prioritization Plan must be submitted using Attachment K- State Entity User Requirements. Attachment K-State Entity User Requirements provides general details regarding each current platform.

|  |
| --- |
| NIC Indiana understands and has complied in our response. We have completed and submitted Attachment K with our proposal as required. Additionally, we have provided Attachment *F.9 Implementation State Entity Prioritization Plan* to describe NIC Indiana’s prioritization approach for services not already provided by our team. |

* + - 1. Please confirm your understanding of the SOW creation process and the secondary competitive process as outlined in Attachment J- Scope of Work, Section 1.4.3 (1).and the requirement that all SOW’s must be approved by IOT and the State Entity in accordance with RFP Section 1.4.3, prior to the commencement of work. The State has provided in Attachment P, drafted SOW requirements that will be collected from each individual State Entity during the SOW creation process. The State requests feedback on Attachment P, in the form of modifications, additions, revisions. Please redline Attachment P and submit as part of your RFP response. Please also describe your company’s established process for the creation of individual SOW’s and provide the SOW template and documents utilized during the process. Please include details on the approval hierarchy and time frame for successful creation.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NIC Indiana has read, understands, and will comply with the secondary competitive process outlined in Attachment J. As instructed, NIC Indiana has provided redlines to Attachment P and submitted those as part of our response to this RFP.  Please see the attached *F.5 SOW Template* file for NIC Indiana’s current SOW template for the creation of individual SOW’s.  Typically, SOWs are developed using the following methodology. Time to complete the documents varies based upon complexity of the project but are typically completed within two weeks.   |  |  |  |  | | --- | --- | --- | --- | | **Phase** | **Description** | **Output** | **Responsibilities** | | Pre-SOW Meetings | Develop common understanding of project scope and preliminary timeline. Focus on defining agency needs and expectations. | Meeting minutes with action items | NIC, Indiana representative | | SOW Request | A SOW Request is created that provides a high-level overview of the project, timelines, responsibilities, processes, risk assessment, critical success factors, and marketing initiatives. | Completed SOW Request | NIC assists. Agency develops State Entity SOW. | | Review SOW Request | Analyze State Entity SOW Request, provide functional, non‐functional, and technical specifications.  Application analysis meetings with appropriate agency and NIC staff. Topics may include security, reporting, transition requirements, user interface, reconciliation requirements, legacy system interface session data definitions, or other topics. | Analysis of State Entity SOW Request | Agency, NIC, and State review. | | Develop Fee Analysis | Perform financial analysis and determine proposed fee and model. The proposed model and fee will also be evaluated by the appropriate governance committee when applicable. | Fee Analysis & Approval | Agency and State review, modify, and approve. NIC provides input. | | SOW Proposal | SOW Proposal is created by NIC from the results of the analysis of the SOW Request and the proposed solution to meet the request. | SOW Proposal (Business Case is part SOW Proposal) | NIC assists Agency. | | SOW Proposal Review | Review the proposed SOW Proposal and recommend approval, rejection, or modification. Provide recommendation for prioritization. | Approved, modified, rejected SOW | Governance entity reviews and approves. | | SOW | SOW created from the SOW Proposal and will incorporate all contractual requirements for the SOW, including invoicing, deliverables, fees | SOW | Agency and NIC jointly draft and execute SOW. | | Project Manage | The approved SOW is managed according to approved approach and timeline. | Project Management Plan updated | NIC manages development of project. Indiana provides oversight. | |

* + - 1. Describe how you evaluate a project and scale your project management methodology to best manage the project based on factors, such as size, criticality and project complexity.

|  |
| --- |
| If awarded this NIC Indiana will establish a separate Account Management team that will be dedicated to administration, evaluation, execution, transition, implementation, and management of NIC Payment Platform projects established through the State Entity SOW process. The team will be empowered to tailor project management processes to scale based on the size and complexity of each State Entity SOW. Additionally, the well-staffed, dedicated team will have leeway to manage human resources across multiple projects and scale size according to Indiana’s needs.  In response to requirement *2.4.6.4* above, NIC Indiana is proposing that we are engaged with participating State Entities during the SOW process to help determine scope, schedule, fee model, and overall project requirements, which will ensure NIC Indiana is prepared to scale resources and tailor methodologies for each SOW.  To ensure efficient use of staff and scalability of project management, NIC Indiana will follow well-documented methodologies that are currently accepted by the State and used across all agencies to manage digital government and payment service initiatives. As discussed, NIC Indiana will utilize both waterfall and agile methodologies within its environment. Each of these methodologies has proven specific benefits to Indiana, align with needs of the State, and provide the most efficient use of resources, while leveraging modern development techniques to implement secure payment services.  This hybrid project management approach will allow the NIC Indiana finance team to allocate resources based on the project scale and complexity. For each State Entity SOW project, NIC Indiana will allocate one project lead, one front-end developer, one ecommerce developer, and one quality assurance analyst. As projects increase in size, additional roles are added as needed. Additional resources of each role will be added to larger engagements as required. The NIC Indiana executive team, including the General Manager and the account management team leadership are aware of each project and play an active role, as needed, throughout the project life cycle. |

* + - 1. Please describe in detail the current training offerings available to the State and your company’s ability to create and deliver customized training at no cost to the State. Please provide examples.

|  |
| --- |
| As discussed in response to requirement *2.4.6.3* above, NIC Indiana possesses the necessary domain expertise in Indiana government, an established payments platform, and a repeatable learning model to train government staff on the NIC Payment Platform. NIC Indiana is acutely aware that training is an important part of providing exceptional services to the state.  For each State Entity SOW, NIC Indiana will establish training plans for the agency and technical resources to provide an overview of the NIC Payment Platform. Typical courses/topics include the following:   * Identifying and cataloging all applications requiring payment services * Identifying all integration points * Understanding financial reports, flow of funds, and reconciliation * Handling chargebacks, refunds, returns, and any other exceptions * PCI Do’s and Don’ts * Conducting integration testing * Prioritizing services and determining transition timelines * Post-implementation support processes   Training materials and courses can be customized for the needs of individual SOWs, at no additional cost.  To properly scope training for each project, NIC Indiana will conduct kick-off meetings after award of each SOW with key project sponsors to determine the appropriate implementation and training schedules. Regularly scheduled, web-based, technical, and security training sessions for staff and administrators for the NIC Payment Platform will also be provided.  Please see *NIC Indiana Attachment 1 - CCP Integration Guide.* |

* + - 1. Please describe your company’s current marketing offerings including samples and examples from current clients.

|  |
| --- |
| Marketing is an essential and often overlooked component of a successful digital government program. Our approach, which has been enhanced over years of serving state needs, is designed to put digital government services directly and clearly in the path of citizens who need to use them. For IN.gov, the goal of any marketing program is to drive higher awareness of the availability of digital services and increase transaction volumes through the digital channel.  In every state NIC serves, our goal is to develop and execute a digital marketing platform that elevates state services in search engine results. Our search engine optimization methodologies have been honed after years of promoting digital government services on search engines such as Google. Our marketing and technology teams stay abreast of constantly changing algorithms and aggressively test new approaches to ensure that our partners’ websites and digital services that provide transactions appear high on the first page of search results. In addition, we deploy best practices honed over the years serving IN.gov – including strong, descriptive page titles, plain language, detailed meta descriptions, and content that is updated frequently.  With more than 25 years of experience marketing digital government services, we have learned some valuable lessons about marketing payment services, including:  1. ***Payments-related marketing is only successful when tied to promoting the use of specific digital services***. Citizens and businesses think in a deadline-driven, on-demand manner, so our marketing efforts are focused on elevating awareness of and driving traffic to digital services rather than just talking about how to make a digital payment to government.  2. ***NIC has a track record of success in building email and digital campaigns to target users of key digital services that include an online payment option***. For example, a 2020 email campaign targeted to Maryland businesses that needed to file annual reports and make payments drove a 41% increase in online filings/payments and attracted 11,000 new business filers to the system – 98% of which made repeat filings/payments in 2021. The following is an example of marketing materials from that target campaign. |

* + 1. **Security**
       1. The Contractor must meet all security, privacy and compliance requirements defined in the Security and Privacy section of Attachment J1- Scope of Work-Security. Please confirm you have carefully reviewed all Security and Privacy Requirements in Attachment J1- Scope of Work-Security.

|  |
| --- |
| NIC Indiana has carefully reviewed all security, privacy, and compliance requirements associated with the RFP, including Attachment J1, and we confirm that our solution will meet these requirements.  NIC understands that we are responsible for the security of the transaction data and processing procedures for our systems and systems within our control and for compliance with all applicable state laws pertaining to the security of transaction data in connection with these systems. NIC security staff supporting the NIC Payment Platform use industry best practices to ensure that the State will remain compliant with all applicable Federal, State, and other laws and regulations.  NIC's commitment to security is unparalleled. Our security program includes a comprehensive suite of information security solutions and controls to support the payment processing operations of every partner. Our proven approach integrates security assessment, monitoring, and management to deliver best-in-class security solutions.  1. Certified by the Payment Card Industry Data Security Standards (PCI-DSS) as a Level 1 Service Provider by a Qualified Security Assessor (QSA)  2. Listed as a PCI-DSS Compliant provider on Visa and MasterCard's Global Registry of Service Providers  3. SOC2, Type 2 audited solution  4. Fully compliant with federal, state, local, and industry security standards  5. Meets all Sarbanes-Oxley compliance requirements  6. NIC is a participating organization of the Payment Card Industry Security Standards Council  7. NIC has multiple PCI certified Internal Security Assessor (ISA) staff to provide the equivalent capabilities of QSA staff for non-QSA companies, and has a QSA company under contract to assess NIC’s payment environment  8. Utilizes a nationally recognized security assessor to provide a third-party security assessment |

* + - 1. The Contractor must adhere to the latest versions of NIST 800-53 and 800-53A standards in their environment. Is the payment processing solution environment you have proposed compliant with the above standards? If your answer is other than 'Y', please describe your current level of compliance, any shortcomings as they apply to this inquiry, and, if applicable, provide a justification as to why Contractor believes this level of compliance is unnecessary. Describe the security control(s) in place to protect data in use and transmission of data to the State Network (keeping in mind requirements related to NIST 800-53). Provide examples where you have implemented these controls in a similar environment.

|  |
| --- |
| Yes, NIC adheres to the latest versions of NIST 800-53 and 800-53A standards. Financial processing is hosted in our high-security payment hosting environments. These distributed hosting environments are located in our private datacenters located in Virginia and Texas. Payment processing hosting environments are purposefully isolated from non-financial services, are certified as PCI DSS Level 1 compliant, and comply with NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Rev. 4 and all applicable IRMs. Our payment processing environment and technologies include comprehensive disaster recovery and emergency preparedness services.  Our security personnel are trained experts in delivering to NIST SP 800-53 security controls and have successfully obtained and continue to maintain multiple Authority to Operate (ATO) certifications with the federal government. NIC implements security controls from the NIST 800-53rev 4 standard and continually assesses these controls using an internal assessment program based on the NIST 800-53rev 4 standards for assessing security and privacy controls. We have contracted partnerships with industry leading third-party security assessors to validate the effectiveness and compliance of our security practices and controls annually, and this includes ongoing assessment activities such as log analysis and application scanning. An annual PCI DSS assessment that NIC has performed on the environment as required by the Card Brands. This assessment is performed by a PCI Qualified Security Assessor (QSA) and a Report on Compliance (ROC) is issued and submitted to the Card Brands annually. The ROC has an Attestation of Compliance (AOC) section that is utilized to demonstrate compliance to customers and partners. The most recent version of this report is provided in a later section as proof of PCI DSS compliance.  Examples  All of NIC’s government engagements must comply with the same set of security standards based on the NIST 800-53 controls and NIC has implemented these controls in numerous, similar government environments across the U.S., including local, state, and federal governments. Specifically, in Indiana, the currently implemented payment solution is compliant with these standards and undergoes an assessment against these security controls. This includes 32 states, 15 federal agencies, including payment processing for Recreation.gov, as well as hundreds of local government implementations. |

* + - 1. The Contractor must provide a system that will encrypt all financial and confidential data transmitted over the Internet compliant with the FIPS 140-2 standards. Please provide a description of your current system, including the version of Transport Layer Security (TLS) that your system supports. Please provide a detailed description of your ability to meet all requirements set forth in Attachment J1- Scope of Work – Security Requirements, Section 1.4.3.2.(1) (c).

|  |
| --- |
| NIC is currently using tools that are FIPS 140-2 compliant for encryption and will continue to ensure these tools securely transmit any sensitive data. NIC also currently uses a NIST approved SCAP tool for baseline configuration monitoring of systems and devices. Use of FIPS 140-2 for encryption is validated as part of our NIST 800-53rev4 assessment program. NIC also maintains an annual PCI Level 1 Service Provider certification for the proposed NIC Payment Platform which also validates encryption protocols as required by the PCI DSS.  The NIC Payment platform supports Transport Layer Security (TLS) version 1.2 and we are in the process of adding support for the recently released TLS 1.3 to our payment gateway. TLS 1.3 provides the highest level of transmission encryption in use on the internet today. Client connections are required to use at least TLS 1.2 and appropriate secure algorithms.  Data encryption of financial information is critical to preventing identity theft. Data is stored for the shortest amount of time required by the business process to complete the transaction. At no time is sensitive authentication data stored such as CVV or PIN codes.  NIC Indiana uses field-level encryption for cardholder data as required by the PCI DSS. This ensures that only authorized applications may decrypt this data, rendering it unreadable should it leave the cardholder data environment. It also ensures that the data is not altered after encryption.  The NIC Payment Platform currently meets all the Section 1.4.3.2.(1)(c):   * All data including backups are retained within the continental United States. * Information is always encrypted during transmission using TLS. * Our hosting facilities and operational procedures incorporate appropriate controls from NIST 800-53 and undergo assessment according to NIST 800-53A * NIST 800-53 security controls protect information in use, in transit, and at rest. * Encryption mechanisms use a FIPS 140-2 cryptographic module and adhere to NIST 800-131A encryption requirements. * Our payment platform supports the option to securely store payment information for the user to add convenience in making future payments. * Access to payment and financial data is strictly limited to only authorized administrative user accounts. * NIC commits to providing the State confidential information upon request and, in consultation with the State, will destroy the data after contract expiration. * All data movement into or out of the State environment will comply with standard State processes. |

* + - 1. The Contractor's Payment Processing Solution must provide a system that has the ability to use Address Verification Services (AVS), Card Verification Value (CVV2), Card Validation Code (CVC2), Cardholder ID (CID), Card Security Code (3CSC), MasterCard SecureCode, and any other fraud prevention tools. Please describe your current ability to meet this requirement.

|  |
| --- |
| The NIC Payment Platform incorporates several fraud-prevention features to minimize and detect fraudulent payments. These include:   * **Address Verification Services (AVS)** – By collecting information about the billing address for the card, the NIC Payment Platform can validate through the credit card processing networks that the person paying knows the correct billing address for the card. The entire address can be validated, but typically only the zip code is validated since validating the street address can falsely indicate a fraudulent payment due to variances in how street addresses are represented. * **Validation of CVV2, CVC2, and CID** – The NIC Payment Platform can process these codes at the time of payment. PCI DSS and card network rules dictate that this code never be stored when processing a payment. By validating this code at the time of payment, the NIC Payment Platform reduces the likelihood that someone without physical access to the card is making the payment. * **3CSC, MasterCard SecureCode Fraud Prevention Codes –** These fraud prevention tactics are 3DS2 and require multifactor for the end user to complete a payment. This technology is not currently supported by NIC, as it is primarily used in Europe where it is needed to comply with the European SCA regulations. NIC will continue to monitor this technology and any regulations that are imposed within the United States. * **Maximum Transaction Limits** – For each service processing payments, a maximum limit on the payment amount can be configured. This minimizes the impact of fraudulent payments if they do occur. * **Real-Time Payment Authorization** – In real-time, the NIC Payment Platform connects to the card acquirer to verify that the card has sufficient funds to make the payment and locks these funds for a period of time to ensure that the funds can be captured during processing of the payment. * **Validation of a CAPTCHA** – CAPTCHA stands for “Completely Automated Public Turing test to tell Computers and Humans Apart." The NIC Payment Platform checkout process incorporates CAPTCHA technologies to prevent automated robots from brute force guessing payment information since each attempt requires intervention by a human.   NIC has algorithms in place to monitor for suspicious activity proactively and reactively. In addition, NIC is currently engaged in expanding our fraud prevention program to include targeted machine learning and artificial intelligence specific to chargebacks on certain high-risk services. Though we are in the early stages of this effort, the NIC models have been able to predict chargebacks for these services with an 80% accuracy rate. The team will continue to hone this proactive mechanism as well as integrating other data analytics driven fraud prevention measures, such as 3DS in the future. |

* + - 1. The Contractor's Payment Processing Solution must provide a system that is protected by security, using a public certificate authority to ensure that connected clients are on the Contractor's system. Please describe your ability to fulfill this requirement.

|  |
| --- |
| NIC Indiana already fulfills this requirement. Certificates used by the NIC Payment Platform to enable TLS encrypted transport connections are issued and certified by a leading third-party certificate authority. These certificates provide assurance to clients that they are connecting to the actual payment platform and that their connection has not been hijacked or intercepted. Furthermore, client connections to the NIC Payment Platform are authenticated using either client certificates or through service account credentials transmitted as part of the API call. |

* + - 1. The Contractor's Payment Processing Solution must have the capability to store client payment information, i.e., card info, account detail, etc. with ability to configure payment center to not allow this or provide it on an opt-in basis to clients to meet prevailing State of Indiana standards and policies. Please provide your ability to allow clients to opt in or out of this solution feature.

|  |
| --- |
| NIC Indiana and the NIC Payment Platform never store payment information without the explicit consent and opt-in of the user. If the user wishes to store payment or account information for increased convenience in making future payments, they will explicitly select this option during checkout and their information will be securely stored using the NIC Payment Platform’s Wallet API. Each service integrated with the payment platform can choose to allow or disallow the option to store payment information during the checkout experience.  Wallet API  Using the NIC Payment Platform’s Wallet API, front end applications can implement credit card management and payment processing features without exposure to PCI data. PCI data is submitted via iFrame views delivered to the end user browsers from a web application that works in coordination with the Wallet API. This makes front-end applications easier to design, build, maintain and update without impact to the payment processing component. The reliability, security, and ease of integration of the Wallet API allows the front-end application to define and control the user interaction.  Wallet API works with the client’s existing authentication method to provide stored payment methods. No authentication is required for one-time non-saved payment processing.  Benefits Include:   * Removes Risk and Liability * API Integration * Reduces development time and cost * Account Management * Uses stored or non-stored payment methods * PCI DSS Compliant   Advanced or Recurring Payments  The NIC Payment Platform supports the capability to establish recurring and installment billing for credit/debit cards and ACH. The solution is modular based on the responsibilities of the calling applications. However, all implementation options rely on leveraging NIC’s wallet functionality, to securely collect and store the user’s payment information, but the calling application may or may not choose to be responsible for the user interface for the user to setup and manage the payments or for a customer service agent to manage payments on behalf of a user.  If the calling application maintains the authentication and experience of a user, then the application would interact with NIC’s wallet service via a REST API (and iFrame) to collect and store the user’s payment information in NIC’s secure PCI vault. Once the payment information is stored in the vault, then the calling application is provided with a token to identify the payment method to be leveraged for future transactions. The agency in this case would leverage this token to make payments based on a schedule that the agency calling application is maintaining.  If the agency prefers a more integrated approach, then the calling application can re-direct the user to NIC’s common checkout, where the user would make their scheduled or one-time payment selections that are available for that specific application. The scheduled and recurring feature is not enabled by default, so this would be configured with the agency when establishing the payment service for each specific application.  When utilizing the fully integrated approach, NIC will leverage our Citizen Experience platform, Gov2Go to manage the user authentication to access their stored payment methods, as well as manage and edit their current selections. The calling application will leverage the fully hosted common checkout to provide the details of the transaction to NIC and NIC will leverage a postback method to provide the calling application with details of the payment setup, schedule, updates to a schedule and notification of a payment made for each instance. |

* + - 1. The Contractor's Payment Processing Solution must be Payment Card Industry Data Security Standard (PCI DSS) compliant based on the most current version of the standards. Please provide a detailed description of your company’s ability to meet all Payment Card Industry (PCI) security standards as outlined in Attachment J1- Scope of Work- Security Section 1.4.3.2.(1).(b). Please confirm if your payment processing uses tokenization. Please provide solution names and details regarding the PCI certifications the solution has been approved for. The Respondent shall also submit the PCI certification letter, from a qualified security assessor company. This certification letter must be dated no earlier than 12 months prior to the RFP Response date outlined in RFP Section 1.8.

|  |
| --- |
| The proposed NIC Payment Platform solution is fully compliant with all PCI DSS security requirements, including those outlined in *(b) “Security: Payment Card Industry (PCI) Data Security Standards”* of *Attachment J1- Scope of Work- Security Section 1.4.3.2.(1).(b).*   * Cardholder data is encrypted at the point of interaction such as at the Point-of-Sale system card acceptance device and mobile card swipe peripherals. * Cardholder data stays encrypted as it is transferred to the NIC Payment Platform where it is decrypted and processed. * All card acceptance devices are preinjected with encryption keys and secure practices are used for managing these devices. * The environment where cardholder data is decrypted is a high-security environment that undergoes continuous security monitoring and frequent security assessment against PCI DSS requirements and NIST 800-53 controls. * Only secure, strong encryption technologies are used and NIC follows mature practices for key management according to accepted industry best practices.   PCI DSS Compliance  The NIC Payment Platform was built specifically for the needs of government and has evolved over two decades of real-world usage to be the most functional and reliable payment processing and financial management technology available to government. The NIC Payment Platform is hosted in high-availability, high-security Evoque datacenter facilities administered by NIC. PCI DSS Level 1 compliance is maintained for both the hosting environment and the payment software itself. All payment processing for Indiana will use the NIC Payment Platform gateway, including processing of credit card, debit card, and e-check (i.e., ACH) payments through online, IVR, point of sale, mobile, and alternate payment channels.  NIC Services, LLC ¾ the peer NIC subsidiary that provides and operates NIC’s PCI compliant Payment Platform (NIC Payment Platform) for NIC and all its subsidiaries, including NIC Indiana ¾ is certified as a PCI DSS Level 1 Service Provider and listed on Visa's Global Registry of Service Providers and the Mastercard SDP Compliant Registered Service Provider List.  NIC and the NIC Payment Platform undergo an annual PCI DSS Level 1 Service Provider assessment from a Qualified Security Assessor (QSA) certified by the PCI Security Standards Council (PCI SSC). In addition, the NIC Payment Platform annually undergoes a SOC 2 audit producing a SOC 2 Type 2 Report that covers the Security, Availability and Processing Integrity Trust Principles over NIC’s Payment Processing Applications.  NIC also supports a suite of validated Point-to-Point encrypted card-present solutions, to mitigate scope of our government partners who handle transactions in-person, over the phone, in a mailroom or any other situation where the cardholder is providing the agent with sensitive data.  Tokenization  Our solution stores a Fiserv TransArmor token at the initial pre-authorization of the debit/credit card. TransArmor is a dual-layered payment card security solution that combines software- or hardware-based encryption with tokenization technology. The solution secures the transaction from the moment of swipe or card not present entry – prior to transmission and throughout the payment process – with encryption. The terminal will send the encrypted transaction to Fiserv and receive the results of the authorization with a token that can be used in place of the payment details. TransArmor tokenization prevents card data from being stored in the merchant’s card data environment (CDE) since the system can store the token instead of the payment details.  PCI Proof of Certification  NIC Services provides payment processing and gateway services for all of NIC’s contracts that require payment services. NIC Services is listed as a PCI-DSS Compliant provider on Visa and MasterCard's Global Registry of Service Providers:   * VISA: <https://www.visa.com/splisting/searchGrsp.do> * MasterCard: <https://www.mastercard.us/content/dam/mccom/global/documents/Sitedataprotection/site-data-protection-pci-list.pdf>   NIC provides and will continue to meet PCI compliance for all of our payment processing clients. NIC Services and the NIC Payment Platform undergo an annual PCI DSS Level One Service Provider assessment from a Qualified Security Assessor (QSA) certified by the PCI Security Standards Council (PCI SSC). The following pages are taken from NIC’s most recent Attestation of Compliance from and signed by a qualified security assessor company. |

* + - 1. Is the Payment Processing solution cloud hosted? If so, please complete Attachment M- IOT Cloud Provider Questionnaire.

|  |
| --- |
| NIC Indiana’s proposed solution is **not** cloud hosted. Since Attachment M is a required submission, we have completed *Attachment M* with N/A for the cloud items and submitted it with our proposal. |

* + - 1. Please describe the type of compliance reports that you have created and generated for client use at the conclusion of the audit/self-assessment.

|  |
| --- |
| NIC performs its PCI DSS evaluation through a Qualified Security Assessor certified by the PCI Security Standards Council. NIC receives an Attestation of Compliance from the assessor annually and performs all required ongoing activities to maintain PCI compliance. This attestation can be shared with agencies upon request during the contract.  In most integration scenarios, the client technology (e.g., agency service) will not fall within the scope of PCI DSS since cardholder information is collected by the platform’s common checkout component, greatly minimizing requirements of the agency. As a Payment Facilitator NIC will work with each agency to customize the compliance program based on each specific agency integration scenario. By way of example, the requirements will differ when accepting card present payments versus an agency that is leveraging NIC’s host platform for an e-Commerce only environment. In all cases the agency may need to review NIC provided training material and perform a self-assessment to ensure they are protecting cardholder information in alignment with PCI DSS requirements. For each engagement, NIC Indiana will support the agency as it prepares its self-assessment. NIC can provide a matrix outlining NIC and Agency responsibilities for each payment flow. |

* + - 1. The Contractor must provide a formal, defense-in-depth security strategy that will be used to provide ongoing security for State resources in the Contractor environment, update the strategy on an ongoing basis, and inform the State in writing within thirty days of strategy updates. As part of ongoing security support, the Contractor must inform the State of both offensive and defensive strategies in place in the Contractor environment. Please provide an example defense-in-depth security strategy that is currently being utilized by a customer of comparable size to the State of Indiana. Please include a description of your approach to evaluating and updating your security strategy as security issues arise or standards change. Please describe your approach to testing for security in systems, applications and applicable networks.

|  |
| --- |
| NIC implements a proven layered and modular information security program to protect state and user information and systems. Security is considered at all points in a project lifecycle. NIC utilizes leading third parties to validate our security posture. NIC utilizes a third-party firm to perform ongoing evaluations of all aspects of NIC’s security program across all NIC contracts. Please refer to the attached file *E.5 CONFIDENTIAL Defense-In-Depth Security Strategy*, which was uploaded with the files in response to Attachment E, for our example defense in depth security strategy.  This program provides verification that NIC's information security controls, policies, and procedures have been examined, measured, and validated by an industry leader against a stringent set of control standards using a proven framework. Currently, NIC does its PCI DSS evaluation through a Qualified Security Assessor certified by the PCI Security Standards Council. In addition, our payment platform goes through the NIC Security and Compliance Assessment Program. The program is a continuous assessment and validation process designed to measure and track NIC’s compliance with multiple information security requirements. These requirements are referred to as NIC Common Controls. This assessment is overseen by our nationally recognized third-party assessor.  Highlights of NIC’s security program include:   * Controls based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIC Corporate Security Requirements and PCI DSS * Comprehensive policies, standards, and procedures * Personnel & Security Training * Physical Security – at Data Centers and NIC’s offices * Network Security * Systems Security * Application Security * Data Security * Logical security * Encryption * Audits, Testing and Governance * Detailed Incident Response Policy and Procedures   The diagram is a high-level overview of the layers of NIC’s Security program. NIC implements all appropriate aspects of this model in support of each of our initiatives.  Graphical Overview of the NIC Security Program |

* + - 1. The Contractor must design a solution that adheres to the latest NIST standards and best practices governing management of user accounts. Examples include time-driven auto disablement, account deletion, locking of accounts, maintenance of user profile data following deletion. The Contractor’s solution must integrate with the State’s single sign on solution, Access Indiana, for State Entity user access. Access Indiana requirements can be found in Attachment N-Access Indiana Requirements. The Contractor's portal support approach must allow single sign-on capability to associated State Entity systems (INtax, Uplink, SOS Corporations). Please provide a detailed description of your company’s ability to meet all requirements in Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2 (1)(d)(i). Additionally, please describe the architecture and implementation steps you plan to use to meet Single Sign-On requirements. Will each State Entity manage its own credentialing, or will the Contractor be responsible for providing an authentication mechanism for all systems? Please clearly describe how your Single Sign-On solution will support this.

|  |
| --- |
| NIC undergoes an ongoing security assessment by a nationally recognized third-party security assessor. This third-party and NIC partner to maintain a stringent and proactive security posture for NIC’s services. These annual audits focus on an assessment of our security operations and measure the alignment with industry standards such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4 ‘Security and Privacy Controls for Federal Information Systems and Organizations’.  Account Management & Password Configuration  To ensure seamless integration with agencies, the NIC Indiana finance team will provide staff to create user accounts, which adhere to the password requirements in *Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2 (1)(d)(i)*. As requested, the proposed Payment Platform and skilled NIC security staff will provide the following services and technology functions:   * Enable or disable user accounts * Configure accounts to be automatically classified as Idle after a pre-determined amount of time with no activity, which disables access to the account. * Provide passwords changes for user accounts, when needed. * A solution that enforces password complexity and standards as configured by the administrator. The proposed system is currently configured to meet requirements as defined by State standards and allows for configuration of password complexity rules. * Provides the capability for password encryption before the password is recorded in any data repository. * Ability to store a cryptographic hash of passwords instead of directly storing passwords.   NIC corporate security policy requires all accounts to have an owner assigned to them. Account managers are responsible for requesting permissions and access for the accounts necessary to perform business functions. Modifications of group memberships and account permissions are performed in accordance with NIC Corporate Security policy. Approval from management and security operations is required for all account creation and modifications. NIC corporate security policy requires access be granted based on least privileges needed to accomplish the business functions assigned and requires separation of duties between developers of applications and administrators of production environments.  Account usage is monitored through central log consolidation to a SIEM tool for analysis and alerting by the security operations team. User Behavior Analytics (UBA) approaches are used to analyze the data in the SIEM tool to identify patterns of traffic caused by user behaviors, both normal and malicious. Read-only access to log information maintained by the SIEM product is restricted to operations and NIC security staff. The SIEM can store and maintain event logs for security related activities for any contractually defined period.  Single Sign-On Solution  NIC Indiana has been a key partner in the development and deployment of Access Indiana for the State, and is highly experienced with the OpenID Connect integration process for third-party products and services. NIC will work with the state to integrate Access Indiana into its products as requested and when applicable, including access for State Entity users into the reporting and administration modules. |

* + - 1. The Contractor shall host a secure SFTP site on which the State can place end user load files. The Contractor’s standard method of data transmittal shall be through the exchange of flat files via a secure SFTP process, allowing the transfer of files between two sites using the Internet’s TCP/IP protocol. Utilizing SFTP, the State and Contractor shall exchange files securely via the Internet or a private network (Extranet). Please provide a detailed description of your company’s ability to meet all criteria as set forth in Attachment J1 – Scope of Work- Security Requirements, Section 1.4.3.2.(1).(d).(ii).

|  |
| --- |
| NIC Indiana understands and will comply. The proposed solution will meet all of the requirements of *Attachment J1 – Scope of Work- Security Requirements, Section 1.4.3.2.(1).(d).(ii)*. NIC currently hosts a secure SFTP site to allow the State to place end user load files and will continue to do so. The proposed NIC Payment Platform provides the capability to transmit data through flat files via a secure SFTP process, using TCP/IP protocol.  Our current SFTP solution provides:   * Secure, automated exchange of financial data * Safeguards against unauthorized access or manipulation of State data through encryption and protected upload areas * Cost-effective file transfer * NIC Indiana’s superior service and support |

* + - 1. The Contractor must have in place a Privacy Program with a designated single point of contact for all privacy matters (comparable to a Chief Privacy Officer, Vice President of Privacy or similar). Please provide a detailed description of your company’s ability to meet the Privacy requirements set forth in Attachment J1- Scope of Work – Security Requirements, Section 1.4.3.2 (1)(e). Please include an example Privacy Program that your company has established for a client of comparable size to the State of Indiana.

|  |
| --- |
| NIC understands and will comply. NIC implements security controls from the NIST 800-53rev 4 standard and continually assesses these controls using an internal assessment program based on the NIST 800-53rev 4 standards for assessing security and privacy controls. NIC Indiana’s privacy program reflects industry best practices for privacy programs.  Protecting the confidentiality and integrity of data, whether it originates from the individuals or from a government system, is of utmost importance to NIC. NIC employs a comprehensive security program to protect data at all points within the infrastructure. Data governance is a substantial element of the security and privacy program. The data governance plans and supporting activities determine how data is classified, secured, retained, and destroyed including controlled user access to all PHI and PII to those with a job-related need for access and not storing any PII without approval from the state. NIC’s data governance approach incorporates the use of privacy-by-design tools as part of our Privacy Program, including using data de-identification for adequate PII and PHI protection when required. NIC Indiana and NIC as a whole securely provide thousands of applications that collect PII such as payment data and PHI, including managing health systems such as Prescription Drug Monitoring Programs.  These approaches are in compliance with current State laws, Federal laws, and IT security standards including Indiana Code 4-1-6 is the State’s law regarding Privacy of Personal Information on systems maintained by the State.  Upon the start of the contract and annually thereafter, NIC will conduct a security and privacy review in accordance with State guidance ensuring compliance as well as provide continuous monitoring of security controls for the entirety of the contract. In addition, NIC will perform a Privacy Impact Assessment (PIA) for each system containing a State application that contains PII. NIC Indiana will also reasonably facilitate the State’s compliance with IC 4-1-6, which requires state agencies to report on systems that collect PII.  NIC will provide a privacy policy notice and link to the details of this policy. Our privacy policy will demonstrate that we value their privacy, how we protect their information, and how their information is used. This privacy policy is compatible with the State’s own privacy policy.  Additionally, NIC designates Jayne Friedland Holland, NIC’s Chief Security Officer and corporate legal counsel as the single point of contact for all privacy matters. Jayne provides the following certifications: Certified Information Privacy Professional (CIPP), IAPP Certified Information Privacy Manager (CIPM), PCI Internal Security Assessor (ISA), and Payment Card Industry Professional (PCIP). She is supported by her team, the NIC Corporate Security Team, which employs veteran cybersecurity professionals who provide security oversight of security operations across NIC and staff with the skill level necessary to ensure compliance by the Contractor in use of this information and in reporting requirements. Technical leadership for this team is provided by:   * Rodney Caudle – Director of Information Security * CISSP - Certified Information Systems Security Professional * GIAC Security Leadership Certification (GSLC) * GIAC Security Policy and Awareness (GSPA) * GIAC Leadership (GLDR) * GIAC Certified Project Manager Certification (GCPM) * Cryptography I * GIAC Gold Research Paper * GIAC Certified Forensic Analyst (GCFA) * GIAC Certified Incident Handler (GCIH) * GIAC Certified Intrusion Analyst (GCIA) * GIAC Penetration Tester (GPEN) * GIAC Reverse Engineering Malware (GREM) * GIAC Security Essentials Certification (GSEC) * GIAC Systems and Network Auditor (GSNA) * GIAC Web Application Penetration Tester (GWAPT) * Rob Harvey – Lead Security Analyst * CISSP - Certified Information Systems Security Professional * PCI Internal Security Assessor (ISA) * Payment Card Industry Professional (PCIP) * Naheed Bleecker – Director of Privacy Compliance * IAPP Certified Information Privacy Manager (CIPM) * ISACA Certified Information Systems Auditor (CISA) * ISACA Certified Information Security Manager (CISM) * ISACA Certified Data Privacy Solutions Engineer (CDPSE) * ISO 27001 Lean Implementer * Six Sigma Black Belt * PMI Project Management Professional (PMP)   In the event there is a security incident, NIC Indiana follows established processes identified by NICs Corporate Security policy and Incident Response Plan. NIC maintains a comprehensive and confidential Incident Response Plan at a corporate level that includes active participation by NIC’s Corporate Security Team and documents the necessary steps and actions required to be taken in the event of a security incident. Contained within this plan are the necessary steps and requirements for notification of state partners, law enforcement entities, affected parties, etc., where appropriate, and in accordance with applicable state and federal standards, policies, and laws. NIC has included its confidential, and proprietary incident response plan as attached file *F.6 CONFIDENTIAL Privacy Incident Response Plan*.  With a potential security incident, timing is everything. It is imperative that the vendor and the state are prepared in advance, so the team is not figuring it out as the situation unfolds. One way to do that is to have a comprehensive Incident Response Plan and Incident Response Team. Some of the key activities that our Incident Response Plan includes are:   * Defining what types of events or incidents that activate the plan * Establishing team members * Designating roles and responsibilities * Establishing timelines for notification and communication * Testing the plan annually and modify where appropriate * Training employees on the process |

* + - 1. The Contractor must provide a solution that keeps a secure, electronically-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records of note; with the audit trail capable of providing ability to view the data before the change, as well as the new information and information concerning who made the change. Please provide a detailed description of how your company’s solution will meet all the security audit requirements set forth in Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2(1)(g).

|  |
| --- |
| NIC understands and will comply with the requirements set forth in *Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2(1)(g)*. NIC provides robust audit features to log, time stamp, report, review, and appropriately escalate security activity when necessary. Security and user event information is stored and consolidated in a SIEM tool for analysis and alerting by the security operations team. User logging includes a time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records of note. NIC utilizes scenario-based alerts on the data to identify suspicious activity. The NIC customer support team gathers information to investigate the security issue and logs the issue in the IT Service Management tool to preserve evidence of the issue. NIC will retain audit trail history in the SIEM tool for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).  The NIC Payment Platform central repository of transactions allows the agency to integrate efficiently with backend processes, as well as to adhere to industry‐standard accounting and audit processes. NIC has and will continue to engage a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants (“AICPA”) for a System and Organization Controls for service organizations (“SOC”) Type II audit annually for our payment processing environment. NIC Indiana will provide the State with our and our subcontractor’s annual audit report, in compliance with the subcontractor’s confidential disclosure requirements, and submit corrective action plans to the State for any issues included in the audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. |

* + - 1. Please provide a detailed description of your company’s ability to meet all requirements security requirements regarding processing environment testing and vulnerability set forth in Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2 (1)(h). This narrative must include specific details on all required assessments, monitoring plans, vulnerability scans, penetration tests, Cybertrust Security Enterprise Certification, and required certifications. Please also provide a detailed listing of the Intrusion Detection and Intrusion Prevention, and Distributed Denial of Service (DDOS) products that will be utilized as part of the State of Indiana payment processing solution.

|  |
| --- |
| The NIC Vulnerability and Remediation Standard for the NIC Payment Platform is composed of the following phases:   * A system or application vendor announces vulnerability and resolution information * Security Operations ensures the vulnerability scanner downloads the appropriate plugins to detect the announced vulnerability. * Administrators and Security Operations review vendor announcements * On a monthly basis, Administrators record all changes in the IT Service Management tool required to remediate vulnerabilities or record that no remediations are applicable. * On a monthly basis, Security Operations ensures that the vulnerability scanner finds new vulnerabilities impacting the infrastructure. * Administrators remediate vulnerabilities. * Security Operations ensures that the vulnerability scanner detects the remediated vulnerabilities. * Security Operations reports the status of Vulnerability Management to NIC Management.   In accordance with the related security requirements set forth in *Attachment J1- Scope of Work- Security Requirements, Section 1.4.3.2 (1)(h)*, NIC currently meets and will continue to provide all of the stated requirements, including the following:   * An initial self-assessment within three months of contract execution and a formal security risk assessment of the Contractor's environment, with a strategy and action plan to address identified risks. * Continuous monitoring, based on NIST 800-137 guidance. * Continuously monitor and provide to the State real-time, up-to-the-minute threat intelligence, including strategic (through recognized national and global security sources) and tactical and operational/technical intelligence. NIC will communicate in writing any changes to the threat landscape that could impact the State of Indiana and include advice on action to be taken by the State if required. * Perform quarterly internal and external vulnerability scans, using PCI Approved Scanning Vendor for external quarterly scans. * Perform annual penetration test and provide results to the State. * Annually provide the State with evidence of a certification from a nationally recognized security assessor similar to Verizon Cybertrust. * Use Intrusion Detection and Intrusion Prevention products to help identify and report intrusions to NIC staff in order to take immediate countermeasures. * IRS IV & V certification, if applicable. * Remain equipped with such advanced intrusion detection appliances as event correlation, packet filtering, and denial of service defense or its equivalent. * Maintain multiple layers of security devices, firewalls, and Web application firewalls, and load balancing capabilities. Provide ability to use AVS, CVV2, and other fraud prevention tools. |

* + - 1. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations (“Business Continuity Requirements”). Please provide an example of the Business Continuity plan that your company has in place for a client of comparable size to the State of Indiana inclusive of all instructions and procedures. Provide clear explanation of where your Disaster Recovery approach differs from that prescribed by the State. Please review the following State of Indiana Disaster Recovery site and confirm that all requirements are included in your company’s documents/instructions/procedures: <http://www.in.gov/iot/2336.htm> Please outline any State requirements that are not included in your current plan and how they will be incorporated.

|  |
| --- |
| NIC has formal disaster recovery (DR) and Business Continuity (BC) plans for the NIC Payment Platform and will create a specific plan for the services in Indiana that utilize this solution. The plans are verified on a periodic basis, based on the specific needs, by conducting DR tests that exercise the key components of the recovery plan, which typically include restoration of data, network confirmation/configuration, and application certification. Please refer to the attached *E.4 CONFIDENTIAL Disaster Recovery Bus Continuity Plan*, which was uploaded with the files in response to Attachment E, for our example Business Continuity Plan.  NIC will work closely with Indiana to plan and execute the DR testing. In the event of an actual declared emergency, the verified DR plan is executed in the production environment in the same manner as certified during testing. NIC manages and supports DR/BC plans for all state partners, programs for federal agencies and countless local government entities.  The NIC Payment Platform is hosted at two geographically separated Evoque (formerly AT&T) Internet Data Centers (IDC). The platform was architected to use a dual data center architecture for fault tolerance and to support mission critical systems. At any given time, the two facilities for payment processing may be active for different payment processing services. The geographically separated datacenters are configured in a hot/hot setup. This is accomplished through a combination of fully redundant systems, database replication and global traffic management. If there is a service outage or degradation at the primary facility for Indiana, services in the alternate datacenter are online and immediately available to handle transaction activity once traffic is directed to the alternate site.  At any given time, the two facilities for payment processing may be active for different payment processing services. This is accomplished through a combination of fully redundant systems, database replication and global traffic management. The two IDCs were selected in separate geographic areas to support the business in the event of a disaster or emergency. Not only is the NIC Payment Platform prepared for disaster recovery of mission critical services, additional proactive activities can take place with little downtime. NIC frequently utilizes the dual data center architecture to perform maintenance and to quickly respond to other situations requiring service relocation such as service impairments and performance degradations.  NIC has developed a comprehensive disaster recovery plan to restore business services within 24 hours of declaration. NIC's disaster recovery plan is intended to:   * Provide an organized and consolidated approach to manage response and recovery activities following any unplanned incident or business interruption, avoid confusion, and reduce exposure to error. * Provide prompt and appropriate response to any unplanned incident, thereby reducing the impacts resulting from short-term business interruptions. * Recover the business functions in a timely manner, reducing the time during which NIC is unable to conduct business. * Recover information systems and data network environment in a timely manner, increasing the ability to recover from a damaging loss to the facility. * The recovery strategy utilizes recovery computers and workspace at an alternate recovery facility to recover business functionality.   NIC Indiana currently operates data center facilities under its current contract with the Indiana Office of Technology. Our DR strategy meets or exceeds the state’s requirements specified at <http://www.in.gov/iot/2336.htm>, and NIC Indiana has successfully executed DR testing plans in coordination with IOT over the past 6 months. |

* + - 1. Does your solution provide capability for password encryption that is FIPS 140-2 compliant before the password is recorded in the data repository? Please describe the various types of encryption used for data at rest, specifying by data type (PII, PHI, other sensitive data). Describe how/when encryption is applied (using data flow or process flow diagrams).

|  |
| --- |
| Yes, the NIC Payment Platform provides capability for password encryption that is FIPS 140-2 compliant. This is a requirement of our NIST 800-53 aligned security program and is a validated control.  NIC Indiana protects the confidentiality of data at all points within the systems and for the entire lifecycle of the data. NIC Indiana employs a comprehensive Security Program to protect data at all points within the infrastructure. Data governance is a substantial element of the Security Program. The data governance plans and supporting activities determine how data is classified, secured, retained, and destroyed. These approaches are in compliance with Indiana State law and IT standards.  Encryption is a critical component of our security strategy and a variety of encryption technologies are incorporated throughout our security architecture:   * Transport Layer Security (TLS) version 1.2 is used for transport security which employs a variety of strong, modern ciphers to encrypt information exchanged between clients and users of the NIC Payment Platform. We are in the process of upgrading our transport encryption to TLS 1.3 which was recently finalized. * Sensitive data collected by the platform is encrypted in the database when at rest using Oracle’s TDE encryption and additionally encrypted in database backups. * Cardholder data is encrypted Point-to-Point from point-of-sale card acceptance devices to the NIC Payment Platform using encryption technology built into the card acceptance devices. * Cardholder data is tokenized using Fiserv TransArmor and/or using our internal encryption technology - FutureX. * Using a FIPS compliant encryption module, government user passwords are either encrypted or hashed using modern cryptographic algorithms. * Communications with card acquirers like Fiserv are always encrypted using transport encryption, file encryption, or both. * ACH files are encrypted using RSA encryption before transmission to the bank for processing and bank return files use similar file encryption.   To further clarify how encryption is used to protect cardholder data and PII/PHI during a payment transaction, NIC has included four flow diagrams, each pertaining to a different category of payment transaction.  Online Credit Card Payment Flow Encryption    Online ACH Payment Flow Encryption    Over-the-Counter Payment Flow Encryption    Mobile Field Payment Flow Encryption |

* + - 1. When creating applications for clients, in the application design, where does the application store application security data (such as user accounts, security policies)? Please describe your approach/process.

|  |
| --- |
| NIC protects the confidentiality of application data at all points within the system and for the entire lifecycle of the data. Users of applications created for clients access the systems by authenticating through a single sign-on solution. The single sign-on solution streamlines username and password management and protects user identities in a centralized location. It also offers client applications a single point of integration with a community of users that are an amalgamation of citizen and business identities as well as identities from trusted federated domains. NIC Indiana applications maintain user profiles linked to the centralized identities for storing application-specific user settings as well as the user's role and/or privileges within the system. The roles, privileges, and other domain-specific user data within the application are used in the security policies to restrict access to modules, features, or actions in the system. The security policies are implemented into the system itself according to the business rules whereas application behavior control settings and user role- and group-membership as well as user privilege assignment are persisted within the data store of the system. |

* + - 1. Please describe any instances where Contractor applied data de-identification on behalf of a client.

|  |
| --- |
| As a trusted state partner for more than 26 years, NIC Indiana is very familiar with the need to extract data from systems and apply data de-identification tactics in order to repurpose the data for various reporting needs. Specific to this payment opportunity, NIC Indiana has extracted detailed transaction data, applied de-identification, and provided copies of the data to the State for analysis and review. The most common occurrence of this type of request is to analyze payment metrics and trends across the enterprise payment program.  When data de-identification is necessary, appropriate resources such as NIST IR 8053 De-Identification of Personal Information or HHS.gov's guidance regarding methods for de-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule will be consulted. |

* + - 1. Please describe any instances where security root cause analysis was utilized on behalf of a client.

|  |
| --- |
| Root-cause analysis is important in any business especially where technology is concerned. As a result, NIC Indiana strives to find the root cause in order to fix the problem wherever possible, rather than just fixing the immediate incident. An example of how we do root cause analysis is with respect to one of our network carriers, Level 3. Level 3 had an issue where service had been degraded causing the state portal to timeout and become very sluggish when serving up content. The portal is n-carrier redundant at the data center, but this means that all carriers are in use, thus Level 3 was still impacting the core business. Identifying this as a problem, we went to work architecting a better network solution. Working with Expedient we created a new solution that increased the amount of bandwidth the portal can process tenfold, while increasing the redundancy of the network carriers. While this was a complex and labor intensive task, it was necessary to improve service reliability and ensure future performance needs.  Another example of NIC Indiana examining the root cause to better the portal can be found from several security events that occurred in 2015. Starting in the Spring of 2015, several state portals were attacked by a group of bad actors. This group set its sights on the State of Indiana. The IN.gov portal was taken off-line by several DDOS attacks. Understanding that security is paramount, the portal had already evaluated several DDOS mitigation strategies. As a result, the portal was able to quickly purchase, install, and test a DDOS mitigation appliance within 36 hours of an attack. Shortly after install, the device was put to the test by a bad actor and the attack was mitigated as planned. This is a great example where forward thinking on NIC Indiana’s part and root-cause analysis resulted in a more secure and robust portal. |

* + - 1. Please describe your secure login process for payment processing.

|  |
| --- |
| Users securely login to the NIC Payment Platform administrative interface with an assigned account with certain role-based privileges. Access to the NIC Payment Platform’s administrative interface is controlled at the user level, agency level, and service level ensuring users only have access to information for which they have been granted privileges as assigned by an administrator of the platform. The platform’s merchant setup is hierarchical allowing the State to provide role-based security for each participating agency. Agency staff is granted access to support refund and void capabilities, as well as financial reporting and research tools based on their defined role within the hierarchy. Enterprise Managers are given access at the highest level to view reports for the entire program and this may be appropriate for IDOA or OIT staff. The hierarchy structure allows NIC to define the structure to have the concepts of State Agencies or entities and Services, which could be representative of a separation by merchant number. This hierarchical system will give a state agency’s central office access to view and report on individual merchant IDs for any office or division or at a consolidated level across a division or the entire department. In addition, reports can be scheduled on a per agency or service (MID) basis, so they are sent to the appropriate State admins instead of having to retrieve them. |

* + - 1. Please explain your approach to, and provide examples of, security and privacy metrics reporting.

|  |
| --- |
| NIC Indiana works with each client providing appropriate security and privacy metrics meeting the agreed upon acceptable level of risk for the systems involved. Historically, we have provided assessment results from our security assessor, penetration testing results, application security testing results, PCI ROC's, PCI SAQ-D, and other reports as appropriate and requested. NIC Indiana will work with the State to manage security and privacy metric reporting. |

* + - 1. Please describe your companies use of coding security best practices and key secure coding standards used within any development work and/or applications used by your company.

|  |
| --- |
| Security is an essential component of NIC’s development process. Employing experienced developers and continuously educating developers on how to avoid introducing vulnerabilities is critical. NIC regularly offers development staff the opportunity to be trained in security by industry experts specializing in web application security. The project team will actively work with NIC Corporate Security Team resources who provide security intelligence and analytics, security and threat research, security policy management, and legal discovery as part of overall governance. Additionally, we employ industry standard-practices and tools to detect OWASP and other vulnerabilities throughout the development lifecycle and prior to releasing new or modified software into production. In addition, NIC trains all employees annually on the security policy of the organization including its policies and procedures.  Scanning applications for common vulnerabilities during the testing phase of a new service and after any modifications to a service combined with the continuous screening of applications deployed in production allows NIC to proactively maintain a secure environment. NIC uses a leading application security testing tool that allows for an automated and thorough scan of all written code rather than relying on a user to set up a test through the tool’s user interface. Found vulnerabilities in new systems and code updates are remediated prior to promotion to production following NIC’s Risk Ranking Standard. |