ATTACHMENT THREE – REVISION ONE
Technical Requirements Traceability Matrix

Request for Proposal Number 6249 Z1

Bidder Name: Vision 33

Bidders must describe in detail how the proposed system meets the conformance specification outlined within each Technical Requirement. It is not sufficient for the Bidder to simply state that it intends to meet the requirements of the RFP. The traceability matrix must indicate how the Bidder intends to comply with each requirement and the effort required to achieve that compliance.

The traceability matrix is used to document and track the project requirements from the proposal through testing to verify that the requirements have been met. The Contractor will be responsible for maintaining the contract set of Baseline Requirements. This traceability matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The bidder must ensure that the original requirement identifier and requirement description are maintained from the traceability matrix.

How to complete the traceability matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the Bidder.
Requirement	The description of the requirement to which the Bidder must respond. This language is specified in the RFP and must not be modified by the Bidder.
(1) Comply	Bidder must insert an "X" if the system complies with the requirement. Describe in the response how the system meets the requirement. If the system does not comply with the requirement, the Bidder must address the following: 1. Capability does not currently exist in the system, but is planned in the near future (within the next few months) 2. Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the Bidder's standard capability 3. Capability requires an extensive integration effort of more than 500 hours
(a) Core	Bidder must insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications or configuration to existing functionality.
(b) Custom	Bidder must insert an "X" if the Bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	Bidder must insert an "X" if the Bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor or other 3rd party). The Bidder must describe the product, including product name, functionality, and benefits in the response.

TECHNICAL REQUIREMENTS

The following requirements describe what is needed to support DHHS technical project operations.

Each requirement is identified by the following first three characters:

TEC	General Technical Requirements
STN	Standards Requirements
ERR	Error Handling Requirements
DBM	Database/Data Management Requirements
BKP	Backup and System Recovery Requirements
SEC	Security Requirements
DAC	Data Conversion Requirements
PTT	Production, Test and Training Requirements
INT	Interfaces/Imports/Exports Requirements
PER	System Performance Requirements
DOC	System and User Documentation

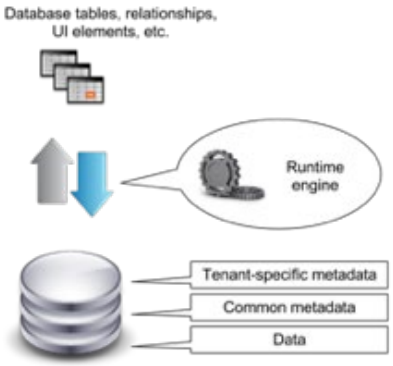
General Technical Requirements

This section presents the overall technical requirements that apply to the software. Describe in the response how the system meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-1	Provide a description and diagram of the technical architecture. Include all database/web/networking hardware, software, tools, etc. Indicate where the system is hosted. Indicate if any components are needed on the client and/or loaded on servers, etc. Solution will only be server/cloud technology in nature. DHHS envisions one domain to be hosted for all applications. Currently, online renewal applications for individuals and businesses subject to the Uniform Credentialing Act are handled by System Automation. Online initial applications for Nursing and online renewal applications for Long-Term Care are submitted via Nebraska Interactive.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:



Our proposed software-as-a-service (SaaS) solution is built on the Salesforce Force.com platform and includes all needed infrastructure, which is fully hosted, managed, and maintained by Salesforce. The BasicGov solution only requires a computer that can run a web browser and an Internet connection or a connected mobile device. No other software or hardware is required. Note that Salesforce applications are delivered on-demand over the Internet, so the City will not need to worry about licensing software or setting up and managing hardware platforms.

The Salesforce Force.com is a modern Platform-as-a-Service (PaaS) that is built for cloud computing, with multi-tenancy inherent in its design. To meet the high demands of its large user population, Force.com's foundation is a metadata-driven software architecture that enables multi-tenant applications.

Force.com combines several different persistence technologies, including a custom-designed, relational database schema, which are innately designed for clouds and multi-tenancy—no virtualization required.

Force.com's core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Force.com's well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others.

Every logical database object that Force.com exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Force.com's Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Force.com does not create an actual table in a database or compile any code. Instead, Force.com simply stores metadata that the system's engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that is required is a simple non-blocking update to the corresponding metadata.

Because metadata is a key ingredient of Force.com applications, the system's runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Force.com uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.

The multi-tenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on "pods." Each pod is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the pod architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's salesforce.com instance from being compromised. This functionality has been designed and undergoes robust testing through an ongoing process by both Salesforce and its customers.

These papers further explain the technology that makes the Salesforce Force.com platform fast, scalable, and secure for any type of application:

https://developer.salesforce.com/page/Multi_Tenant_Architecture

https://developer.salesforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper

https://developer.salesforce.com/page/An_Overview_of_Force.com_Security

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-2	Describe how the system is responsive to mobile technology and works with mobile devices such as smart phones or tablets.	X	X		
Response: The BasicGov platform is fully responsive and will allow input of data on a wide variety of devices, including laptops, tablets and smartphones. The platform goes above and beyond responsive design, however, by enabling the State to have specific page designs for mobile devices, further enhancing mobile optimization. The BasicGov solution only requires a computer that can run a web browser and an Internet connection or a connected mobile device. No other software or hardware is required.					
TEC-3	Describe any third party components that are proposed as part of the system, i.e. using Crystal Reports as a reporting tool.	X			X
Response: 3rd party components may be required for: • Salesforce integration with State's Document Management System (other than Sharepoint) • Creating Service Requests directly from Fax Although, we recommend using Sharepoint for document system avoiding use of any 3rd party application in current phase. Also, we recommend parking the requirement of creating Service Requests from Fax (directly) for next phases.					
TEC-4	Describe how the system is designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic.	X	X		
Response: The BasicGov platform uses a combination of features to ensure that updating business rules is an administrative business function rather than writing code. BasicGov has developed a Global Table approach to ensure that the State can maintain and update common elements in a streamlined fashion. Master Global Tables provides a central location where the State can manage and update reference data for elements such as fees, submission requirements, inspections, and reviews that may be associated with a license application. For example, with an application, you could have several different fee types in a picklist. And for each fee type, there may be many accounting codes tied to it, such as Cash Code, and Receivable Code. Using the Global Table, the State will not be required to maintain individual lists and rules for each individual fee and accounting code In a typical environment, a change to any of these elements would require a re-write of the business rules and processes. With BasicGov, the change needs only to be made to one Master Table record and all dependent business logic will call on the new values once they become effective. BasicGov is built on the Salesforce platform and has a variety of mechanisms to meet complex and simple workflow processes. The Salesforce platform has a selection of tools like workflow, process builder and visual workflow. These are supplemented by the Dynamic Rules Engine (DRE) of BasicGov. The DRE is a criteria-based engine that performs a set of actions in response to a specific event. Records that are processed by the DRE are evaluated against a set of user-defined criteria. If the criteria are met, the Engine proceeds to execute the action. Tasks are easily assigned through the platform and can include email notifications if required. What this means to the State is that workflow processes may be maintained and modified using out of the box tools rather than relying on code to be written.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-5	Describe the upgrade and maintenance process for the system. Downtime and impact to the users must be minimized.	X	X		

Response:

Notification for all BasicGov releases is sent via email to select customer and partner contacts: Monthly Maintenance Release; Quarterly Release; Hotfix Release (Severity 1 issues); Letters Server Release (ad hoc fixes/updates for Letters Server); and, Package Information. BasicGov aims to provide a reasonable amount of notice ahead of time.

For the platform:

Maintenance Schedule

Salesforce generally performs maintenance on Friday evenings, outside of normal business hours (traditionally after 8 PM PST). We can't change our maintenance schedule. Approximately 3 times per year, the site is shut down outside normal business hours for application upgrades. Additionally, between 2 and 4 times per year, the site is shut down outside normal business hours for planned maintenance. Salesforce provides notice at least 48 hours in advance via the Salesforce website as well as notifications upon logging into the State's Salesforce solution. Uptime information is provided in real time on our trust.salesforce.com site.

Updates and Upgrade Process

Major Release Maintenance is for upgrading the services to the latest product version to deliver enhanced features and functionality. Major release dates and times are posted on http://trust.salesforce.com/trust/maintenance approximately one month before release to Sandbox instances. An email notification and blog post regarding Sandbox preview instructions is also sent approximately one month prior to upgrading Sandbox instances. Email notification of major release dates is sent one month prior to upgrading non-Sandbox instances. The Release Notes document describing the new features and functionality is posted in Help & Training one month prior to upgrading non-Sandbox instances. Final release reminders are communicated to all customers approximately one week prior via email and upon logging into Salesforce.

Major release maintenance occurs three times per year. The instance will be unavailable for up to five minutes during the release window.

Patch Releases and Emergency Releases

Used to deliver scheduled and ad hoc application fixes. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday, or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-6	Describe any impact on customizations made to the system for upgrades and maintenance processes. Downtime and impact to the users must be minimized.	X	X		

Response:

Customization made to the system will have no impact to the system for upgrades and maintenance processes. The State will have the capacity to customize the solution to best fit its user's needs. The offers tools for "no compromise customizations," to make it possible to create both fast and easy configuration, as well as deep customizations to meet just about any need. The State can easily customize the Salesforce application through clicks or code methodology. The platform is built on the principal of meeting configuration, development, and administration needs 80% of the time through clicks (configuration) vs. 20% through custom code, dramatically improving cost of ownership and enabling non-technical business users to easily extend existing functionality and/or create entirely new applications that run in the Salesforce framework. Through the point-and-click methodology, custom fields, custom objects, and new applications are easily configured. All customizations are stored as metadata and interpreted at runtime allowing the core code to be upgraded while guaranteeing that customizations will work across upgrades. Below are some of the more typical customizations made by users:

- Customizable User Interface. BasicGov will empower the State to build user interfaces that match its brand, look and feel, and the exact behavior you need and can be done through our declarative development tools (point and click, drag and drop). Users can further augment their individual view through the same point and click process so that they get a solution that is personal and fits their work style.
- Customizable Workflow. The State will have the ability to set up workflow with simple clicks. Automate common operations such as tasks, alerts, data population, outbound XML messages and more without IT support or code.
- Customizable Objects and Fields. New fields, objects, and applications are easily configured in BasicGov. Our point and click, drag and drop methodology enables the State to easily extend existing functionality and/or create entirely new applications that run in the framework.
- Customization of Reports. Customizing reports is as easy as pointing and clicking—enabling the State to react quickly to trends and opportunities as they arise. The dashboard facility will allow the State to build dashboards based on standard or custom reports to present high-level graphical representation of detailed report data. Anyone can build comprehensive reports and dashboards using a wizard-driven reporting engine.

TEC-7	Describe any redundancy built into the system to limit any downtime.	X	X		

Response:

BasicGov is built on the Salesforce platform and, as such, leverages the architecture and redundancy built into the platform. Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that they are the leader in availability. And by making its track record completely transparent, Salesforce proves they are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.

Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status. Detailed historical uptimes are available for existing customers upon request.

This paper further explains the technology that makes the Force.com platform fast, scalable, and secure for any type of application: https://developer.salesforce.com/page/Multi_Tenant_Architecture

TEC-8	Describe how the system has the ability to share data securely, including importing and exporting of data to/from other application software tools, such as a Microsoft Excel file, XML, comma separated value (csv) file, etc.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The State can extract its data at any point in time and retains ownership of their data at all times. The platform offers the following ways to export data: • Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users. • Excel Connector - Salesforce provide an Excel Connector to push and pull data from Excel to Salesforce and vice versa. • Salesforce API - Data can be exported to and from the system though our API at any time or via a number of built in features. • Salesforce Data Loader - The Salesforce Apex Data Loader is a free tool which is used specifically for importing/updating/exporting data in Salesforce. • Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples of these include, but are not limited to, Informatica, Pervasive, CastIron, Boomi, etc. Data can be exported with CRON-like scheduling, or on demand. In the event of an export, all data visibility and record access rules are enforced, and the requestor only obtains the data allowed under the municipality's security policy.					
TEC-9	Describe how the system has the ability to archive data and documents per the DHHS' required record retention schedules, which provides different retention periods for different document types. Describe the method and ability to adjust to changes in the retention schedule.	X	X		
Response: Active customer data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the Recycle Bin. The retention policy for backup media is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). Salesforce customers are responsible for complying with their organization's data retention requirements in their use of the Salesforce Services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may schedule a weekly export of data or copy to a sandbox account. Exports of Customer Data are available in comma separated value (.csv) format by request via Salesforce's Customer Support department. In addition, many exports can be manually pulled by the designated org administrators.					
TEC-10	Describe how the system has the ability to provide audit information on all data accessed or changed within the system.	X	X		
Response: With Field Audit Trail, customers can track changes at the field level for up to ten years and set different policies for each Salesforce object to ensure data is purged when no longer needed. Life sciences companies running clinical trials in Salesforce, for example, can now maintain a complete audit trail of patient data so they can safeguard the integrity of clinical trial results and comply with FDA regulations.					
TEC-11	Describe how the system allows multiple users to use the software applications and database concurrently.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Built on the Salesforce platform, the BasicGov solution can easily scale from one to tens of thousands. Any application that runs on Force.com is automatically architected to seamlessly scale from 1 user to 1,000 to 10,000 users without the customer having to do anything differently. All applications (includes mobile, offline, and read only options) and data running on the platform are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization's mission-critical applications.					
TEC-12	Describe how the system is scalable and flexible enough to accommodate any changes required by the DHHS, or by any federal statute, federal mandate, federal decision or federal policy.	X	X		

Response:

The BasicGov solution is designed with the philosophy of configuration over code. This means that the solution leverages the capabilities of the platform to deliver a highly configurable and unique experience for all of our customers. To achieve the highest value from the solution investment, the State can customize the BasicGov solution to best fit its user's needs. The platform offers tools to make it possible to create both fast and easy configuration, as well as deep customizations to meet just about any need.

Through the point-and-click methodology, custom fields, custom objects, and new applications are easily configured in the platform to personalize BasicGov for DHHS's specific needs. While not exhaustive, the list below describes some of the configurable elements of the platform.

- **User Interface**. The State will build user interfaces that match its brand, look and feel, and the exact behavior you need through our declarative development tools (point and click, drag and drop). Users can further augment their individual view through the same point and click process so that they get a solution that is personal, and fits their work style.
- **Workflow**. BasicGov is designed to ensure that workflow is managed through clicks rather than code. The combination of BasicGov's global tables, Dynamic Rules Engine (DRE) and Salesforce process builders, mean that the State will have the ability to set up workflow with simple clicks. The State can automate common operations such as tasks, alerts, data population, outbound messages and more without IT support or code.
- **Data Objects and Fields.** New fields, objects, and applications are easily configured in BasicGov. The point and click, drag and drop methodology of the platform enables the State to easily extend existing functionality and/or create entirely new applications that run in the framework.
- **Reports**. Customizing reports is as easy as pointing and clicking—enabling users to react quickly to trends and opportunities as the State spots them. The dashboard facility will allow the State to build dashboards based on standard or custom reports to present high-level graphical representation of detailed report data. Anyone can build comprehensive reports and dashboards using a wizard-driven reporting engine.

Salesforce Lightning Declarative Tools

To help IT deliver apps faster, the Salesforce Platform stands alone as the only PaaS that offers Salesforce Lightning, a simple, yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, the State developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Now you can design apps to work uniquely on phone, tablet, laptop, and desktop—all from one place. All while maintaining the flexibility to extend your apps with custom coded Lightning Components for the best of both worlds. Salesforce Lightning Builder tools allow for two vital things no other platform can do: A way for IT to meet business demands faster and become a true partner in driving business forward, and an environment that helps IT manage it all at the pace of business.

Through the flexibility of the platform the State will also have the option to:

- Create full applications with drag-and-drop components including objects, fields, reports, partner components, and page layouts
- Leverage templates and forms for quick deployment
- Visualize and extend your data model
- Quickly add new custom objects, fields, and relationships to your schema
- See details, including field values, required fields, and how objects are related via lookup and master-detail relationships
- Easily automate complex business processes with point-and-click tools
- Automatically update or create new records, emails, and tasks or submit approval requests in a few simple steps
- Visualize the entire process in one place to design and collaborate directly with lines of business owners
- Easily extend processes with flows
- Deploy workflow once, across every device
- Easily connect and access data from external sources with point-and-click
- Create branded public or private communities to connect citizens and businesses that are integrated with your content, data, and business processes

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
• Build, publish, and maintain community portals that work on any device • Easy-to-use tools, templates, analytics, and management allow you to create, preview, publish, and measure changes quickly					
TEC-13	Describe how the system is able to scan, attach, and store different document types (pictures, documents, PDF file, etc.) within the system.	X	X		
Response: Users can upload files, including scanned files, and these will be saved in the Notes and Attachments related list of a record. Assume scanning hardware is provided by the State. Public users may also upload documents as submissions through the application process as well. These submissions will also be stored against the application record.					
TEC-14	Describe how the system has the ability to generate reports and ad hoc queries without performance impact to user access or system response time.	X	X		
Response: The platform includes a reporting engine, designed to allow users to easily create the reports they need. Users can run reports on real-time data or filter to show specific historical data. Rather than relying on a bolt-on, third-party reporting tool, our reporting engine was designed by Salesforce, and is tightly integrated with the security and data model of the platform, which eliminates the problems of managing separate online and reporting profiles. Users create reports using a step-by-step wizard, can schedule when they run, who they are sent to, and can even export report result to Excel if desired. With Report Builder, you can build summary, tabular, and matrix reports and manage filters easily. Report Builder features a drag-and-drop interface to help administrators build complex reports quickly and see changes to you report in real-time. Similarly, a WYSWYG Dashboard builder allows users to quickly create new or customize/copy existing dashboards with ease.					
TEC-15	Describe the help desk operations and support that will be provided with the system.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

BasicGov provides Warranty Support. Functionality that was configured/developed by BasicGov and has unexpectedly stopped working is covered for up to one year from the date of the last BasicGov release date. The combination of subscription renewal and applying BasicGov release updates provides for ongoing warranty coverage. Warrantied items can only be diagnosed by BasicGov. Custom development performed by anyone outside of BasicGov and functionality related to payment processing is excluded from warranty.

BasicGov can provide support through a variety of methods:

- **Online**– BasicGov will provide the State with an online support portal to submit support requests. This is the preferred method of contact and results in the fastest responses to the issue.
- **On-Site**– BasicGov can also provide on-site support to the customer at then current time-and material rates. In addition to these charges, the customer will compensate for associated expenses.

In the Pre–Go-Live phase, BasicGov provides support to those involved in configuring and customizing the overall solution. BasicGov provides advisory and diagnosis, and online training resources directly to the prime lead doing the implementation. In most cases, BasicGov does not undertake any direct configuration; we consult on best practices and help partners get through roadblocks.

Project Support hours are provided to the prime implementation lead until go live, or 18 months from the purchase order date, whichever comes first. Project Support hours cannot be carried forward to any other type of support.

Cloud SynApps provides end to end support right after Project Go-live involving Burn-in Period, Post-Implementation Support and Operations & Maintenance.

Details of the service model, resource plan, SLAs, Contact Process are defined in the proposal.

Standards Requirements

DHHS currently operates its computer system in compliance with many technology and operational standards. These standards originate from internal development, industry best practices and governmental mandates. The Bidder must describe how all applications operate in compliance with these standards and practices.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-1	If web-based system applications are required, describe what industry standard browsers are supported by the system. If the system requires additional components, describe the technical details of those components.	X	X		
Response: The platform currently supports Microsoft® Internet Explorer® , Apple® Safari®, Microsoft Edge, Mozilla® Firefox®, and Google Chrome™.					
STN-2	The system must store data in federally compliant data centers residing within the continental United States of America.	X	X		
Response: Fully supported. Data residency is ensured, and the hosting infrastructure provides multiple venues and redundancy in the mainland USA.					
STN-3	All data is the property of DHHS, and DHHS will retain the exclusive rights of use now and in perpetuity.	X	X		
Response: Fully supported. All data is the property of the client for the duration of the contract term with BasicGov. DHHS may extract its data at any point in time and always retains ownership of their data.					
STN-4	The system must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at: https://nitc.nebraska.gov/standards/2-101.pdf.	X	X		
Response: In its commitment to provide an on-demand enterprise application that is accessible to all individuals, the platform seeks to meet the requirements outlined in the Web Content Accessibility Guidelines (WCAG) 2.0 at Level A. The Salesforce application incorporates several accessibility features that ensure all users have access and can use the application. Many of the features are provided in Accessibility Mode, which can be enabled on an individual user basis. Accessibility Mode can provide a better user experience for users interacting by keyboard only or a screen reader. To help meet the goal of universal design, Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA to the extent possible. The Voluntary Product Accessibility Template (VPAT) is a standardized form developed in partnership by the Information Technology Industry Council (ITI) and the U.S. General Services Administration (GSA) to document a product's conformance with key regulations of Section 508 of the Rehabilitation Act. These documents describe how federal agencies can use Salesforce accessibility features. A third-party vendor has completed an accessibility assessment of Salesforce's core products and has documented their accessibility status using these VPATs. Copies of the VPATs are available on the Salesforce website at: https://www.salesforce.com/company/legal/508_accessibility.jsp					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-5	The system must comply with the sub-parts of Section 508 of the Americans with Disabilities Act (ADA), and any other applicable State or federal disability legislation. Refer to http://www.ada.gov/508/.	X	X		
Response: In its commitment to provide an on-demand enterprise application that is accessible to all individuals, the platform seeks to meet the requirements outlined in the Web Content Accessibility Guidelines (WCAG) 2.0 at Level A. The Salesforce application incorporates several accessibility features that ensure all users have access and can use the application. Many of the features are provided in Accessibility Mode, which can be enabled on an individual user basis. Accessibility Mode can provide a better user experience for users interacting by keyboard only or a screen reader. To help meet the goal of universal design, Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA to the extent possible. The Voluntary Product Accessibility Template (VPAT) is a standardized form developed in partnership by the Information Technology Industry Council (ITI) and the U.S. General Services Administration (GSA) to document a product's conformance with key regulations of Section 508 of the Rehabilitation Act. These documents describe how federal agencies can use Salesforce accessibility features. A third-party vendor has completed an accessibility assessment of Salesforce's core products and has documented their accessibility status using these VPATs. Copies of the VPATs are available on the Salesforce website at: https://www.salesforce.com/company/legal/508_accessibility.jsp				
STN-6	Describe how the system complies with digital signature requirements described in the Nebraska Digital Signatures Act, and all other applicable legal requirements in Nebraska for digital signatures. Refer to http://www.sos.ne.gov/rules-and-regs/regsearch/Rules/Secretary_of_State/Title-437.pdf for definition and standards in Nebraska.	X	X		
Response: Multiple options to meet a 'digital signature' are available to the State. Users access the BasicGov solution using a login/password; in combination with this login procedure an Attestation Page can be configured, and this can suffice as a digital signature. The solution can also integrate with third party electronic signature apps like Docusign using multiple API options. Alternatively, an image file of a signature can be uploaded and merged in documents generated from the system.					
STN-7	The system must comply with all HIPAA and other statutory, regulatory, and policy requirements for protected health information. Refer to http://dhhs.ne.gov/ITSecurity.	X	X		
Response: In provisioning and operating the services, Salesforce complies with the provisions of HIPAA's Privacy Rule and Security and the HITECH Act that are applicable to business associates. Salesforce's customers are still responsible for complying with the same in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service.					
STN-8	If the system requires client software to be installed, describe how the system ensures that all software used for the system can be distributed, installed and configured in an unattended "silent" manner.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The system will not require that client software be installed, therefor this question would be not applicable. Our proposed software-as-a-service (SaaS) solution includes all needed infrastructure, which is fully hosted, managed, and maintained. The BasicGov solution only requires a computer that can run a web browser and an Internet connection or a connected mobile device. No other software or hardware is required.					
STN-9	Current DHHS policies prevent users from making administrative changes and downloading software locally to their PC. Describe how the system supports this policy.	X	X		
Response: The BasicGov solution is a web-based application and therefor will not require the user to download any software to their PC. With regards to administrative changes, the platform can restrict specific users from the ability to make any administrative changes based on their assigned user profiles.					
STN-10	Current DHHS policies recommend not storing any data locally in the event that a user's desktop PC needs to be reimaged (which deletes locally stored data). Describe how the system supports this policy.	X	X		
Response: No data is stored locally. BasicGov is delivered as a software-as-a-service (SaaS) solution and, as such, all data is stored in the Cloud and accessed remotely over the internet.					
STN-11	Describe the report design tools and output formats.	X	X		
Response: The platform includes a reporting engine, designed to allow users to easily create the reports they need. Users can run reports on real-time data or filter to show specific historical data. Rather than relying on a bolt-on, third-party reporting tool, our reporting engine was designed by Salesforce, and is tightly integrated with the security and data model of the platform, which eliminates the problems of managing separate online and reporting profiles. Users create reports using a step-by-step wizard, can schedule when they run, who they're sent to, and can even export report result to Excel if desired. With Report Builder, you can build summary, tabular, and matrix reports and manage filters easily. Report Builder features a drag-and-drop interface to help administrators build complex reports quickly and see changes to you report in real-time. Similarly, a WYSWYG Dashboard builder allows users to quickly create new or customize/copy existing dashboards with ease.				
STN-12	Describe how the system maintains licensed software, including all third-party software, no more than two supported versions behind the latest release, and updated with latest security patches.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: All upgrades, patches, and other system maintenance are provided as part of the subscription service with no additional cost to the State. In addition, both the platform and solution provide 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All users are always on the latest version of the platform because everyone gets instant upgrades (typically in an opt-in basis). Each time Salesforce releases a new version of the platform, the entire community can take advantage of the latest innovations from the product development team. Because of our multi-tenant architecture, Salesforce is able to provide all of customers with a service based on a single version of the platform. Each release will be delivered automatically in a transparent manner and will be tested to ensure it does not break the State's configurations.					

Error Handling Requirements

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ERR-1	Describe the error handling functionality.	X	X		
Response: Exceptions Handling is a mechanism to catch errors and any disrupts of the Normal Flow during Code Execution. Exceptions in Salesforce and BasicGov are implemented in a similar way other Programming Languages such as Java, they use Try, Catch and Finally statement to gracefully recover from an Exception Try: identify the Block of Code in which an Exception can occur. Catch: Block of Code to handle the Exception. It must have an Exception. "Custom Error Message can be concatenated with the System Error to provide a graceful Error to the Users. Finally: Block of code that is guaranteed to be executed. Data Validation Errors are implemented using Validation Rules or Dynamic Validation Rules.					
ERR-2	Describe how the system provides a comprehensive set of edits at the point of data entry to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing (e.g., spell check, zip codes, etc.).	X	X		
Response: Salesforce and BasicGov provide Validation Rules and or Dynamic Validation Rules that allow Administrators to define Data constraints to control the Data that is being added into the System. The validation rules verify the Data entered matches the criteria before saving the Record, if the data entered does not aligned with the Data exception an error is displayed and the system prevents from saving the record.					
ERR-3	Describe how the system ensures all errors are written and categorized to an error log. Describe how the system allows for a user to view, filter, sort, and search the error log.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Debug logs tracks information about transactions. The same Log can also track System.Debug Lines of codes to verify results. Salesforce uses multiple ways to handle exceptions in your code for example using: System.Assert calls, Returning Error Codes or Boolean Values. Errors are captured in a Debug Log There are 3 key components of Salesforce Debug Log: • Debug level: is a set of log levels for debug log categories, such as Database, Workflow, and Validation • A trace flag: includes a debug level, a start time, an end time • A log type: The log types are DEVELOPER_LOG, USER_DEBUG, and CLASS_TRACING Once the Debug Log is set for a user the System tracks any transaction and the Debug log is accessible. The information provided on the Log depends on Debug Level and Log Type. Debug Log is accessible from the Debug Log user interface or from the Developer Console and it allows to filter Data by Debugging entries.					
ERR-4	Describe how the system allows for user-defined alerts of errors, including those to external communication mechanisms (e.g., e-mail and text messaging).	X	X		
Response: When a System Exception occurs, an Automated Email is sent to Admin indicating the nature of the Exception. Also, Salesforce's Workflow Rules and BasicGov's Dynamic Rules Engines support functions that can Trigger an Email Notification of the creation of a Task to alert of errors. The criteria to trigger the Email notification is completely configurable. Additionally, BasicGov has implemented the Concept of Alerts to highlight important information on the Record for certain Objects.					
ERR-5	Describe how the system provides for the generation of standard and customizable error reports.	X		X	
Response: There are no Standard Errors Reports, since the main mechanism to track error is the Debug Log, however; some flag or formula fields can be added to Record to identify an error and build a Custom report that relies on those flags. Example: Formula Field to track Record Completeness (percentage) and create a Report that uses the field as a filter to find records with low level of completeness percentage.					
ERR-6	Describe how the system includes a comprehensive list of error messages with unique message identifiers.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The Salesforce platform that BasicGov is built on and provides a List of Built In Exceptions and Errors: Exceptions: https://developer.salesforce.com/docs/atlas.en-us.apexcode.meta/apexcode/apex_classes_exception_methods.htm REST API: https://developer.salesforce.com/docs/atlas.en-us.live_agent_rest.meta/live_agent_rest/live_agent_rest_error_codes.htm REPORTS: https://developer.salesforce.com/docs/atlas.en-us.api_analytics.meta/api_analytics/sforce_analytics_rest_api_report_error_codes.htm					
ERR-7	Describe how the system displays errors to the user/operator in real-time whenever an error is encountered.	X	X		
Response: Errors are displayed on the Record when the exception occur. A description on the Error is displayed indicating what cause the exception. Additionally, when an exception occurs, an Automated Email is sent to Admin indicating the nature of the Exception.					
ERR-8	Describe how the system has the ability to suppress error messages based upon user-defined criteria.	X	X		
Response: Exception Errors cannot be suppressed, however; you can control how to describe the error. Data Validation errors are only shown if certain predefined criteria is met, which means the error is indirectly suppressed by the criteria and error show if the criteria is not met.					

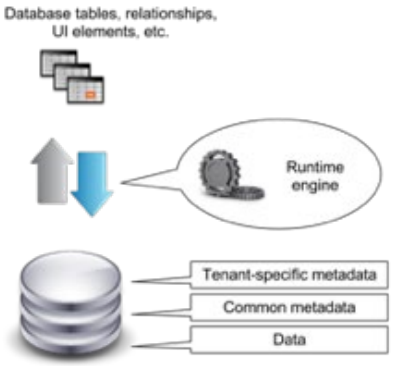
Database/Data Management Requirements

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-1	Describe the database architecture, including the database software that is supported by the system.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:



Our proposed software-as-a-service (SaaS) solution is built on the Salesforce Force.com platform and includes all needed infrastructure, which is fully hosted, managed, and maintained by Salesforce. The BasicGov solution only requires a computer that can run a web browser and an Internet connection or a connected mobile device. No other software or hardware is required. Note that Salesforce applications are delivered on-demand over the Internet, so the City will not need to worry about licensing software or setting up and managing hardware platforms.

The Salesforce Force.com is a modern Platform-as-a-Service (PaaS) that is built for cloud computing, with multi-tenancy inherent in its design. To meet the high demands of its large user population, Force.com's foundation is a metadata-driven software architecture that enables multi-tenant applications.

Force.com combines several different persistence technologies, including a custom-designed, relational database schema, which are innately designed for clouds and multi-tenancy—no virtualization required.

Force.com's core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Force.com's well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others.

Every logical database object that Force.com exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Force.com's Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Force.com does not create an actual table in a database or compile any code. Instead, Force.com simply stores metadata that the system's engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that is required is a simple non-blocking update to the corresponding metadata.

Because metadata is a key ingredient of Force.com applications, the system's runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Force.com uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.

The multi-tenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on "pods." Each pod is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the pod architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's salesforce.com instance from being compromised. This functionality has been designed and undergoes robust testing through an ongoing process by both Salesforce and its customers.

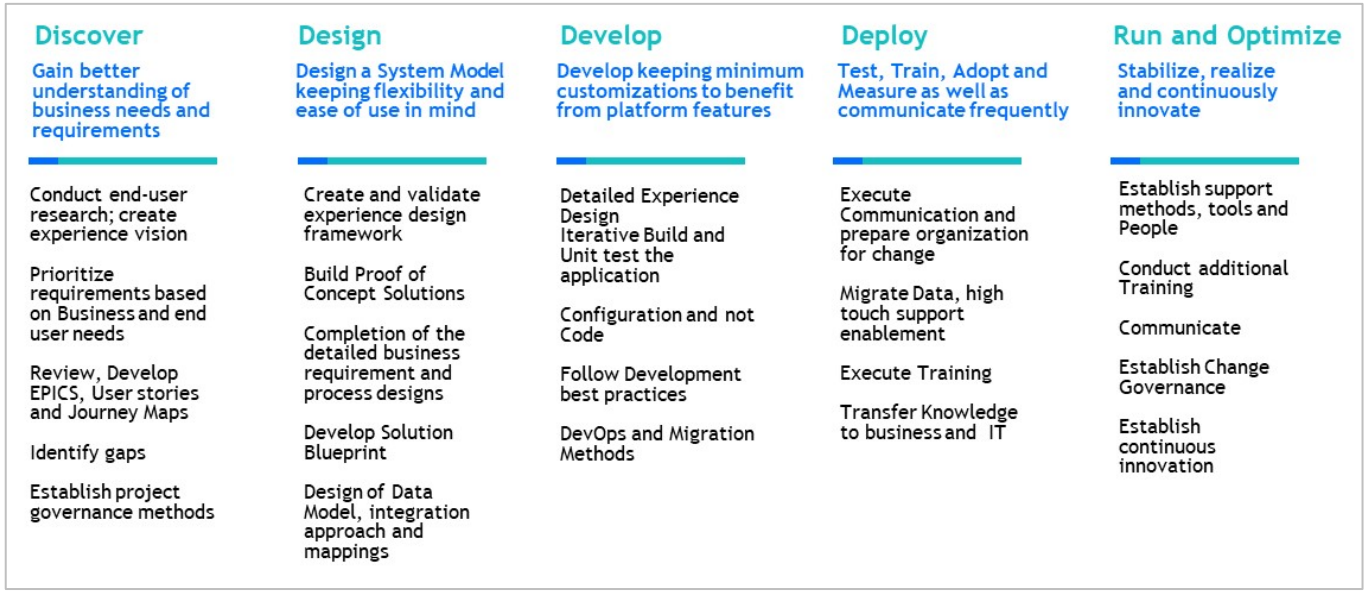
These papers further explain the technology that makes the Salesforce Force.com platform fast, scalable, and secure for any type of application:

https://developer.salesforce.com/page/Multi_Tenant_Architecture

https://developer.salesforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper

https://developer.salesforce.com/page/An_Overview_of_Force.com_Security

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-2	Describe how the system allows changes to be made available immediately on-line.	X	X		
Response: All changes that are made to the production environment are immediately available on-line. The platform allows administrators with specific privileges to make the changes they need to the platform through an intuitive configuration tool. New data objects, record types, fields, user profiles and sharing privileges are among the changes that may be made in real-time. BasicGov does recommend that any changes made to the platform first be tested a in a non-production to ensure it has no effect on production data or workflow.					
DBM-3	Describe how the system facilitates data structure changes to accommodate expanding scope, new services, changing requirements and legislative mandates.	X	X		
Response: The BasicGov licensing model includes a number of custom data objects above and beyond those included with the licensing and permitting solution. These are provided to accommodate expanding scope, changing requirements, new services or any other unknown that may require the platform to be extended. While a specific number of custom data objects is included with the baseline licensing, additional custom object licenses may also be acquired on an as-needed basis.					
DBM-4	Describe the standard software development life cycle (SDLC) for deploying software. Describe the process for planning, creating, testing and deploying the system.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Based on the requirements outlined by the State in the RFP, Cloud SynApps proposes a 46-week plan from Discovery to Deployment (Go-live) to implement the Licensure Information System for State of Nebraska. Details of the work plan and implementation schedule are outlined in the proposal. List of activities to be achieved during each phase of SDLC are outlined in the figure below.  				
DBM-5	Describe how the system provides the flexibility to extract and load data into standard non-proprietary software formats.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The platform provides a robust data loader and backup utility to provide the flexibility to extract and load data into standard software formats. The Data Loader is a client application for the bulk import or export of data. Use it to insert, update, delete, or export records. When importing data, Data Loader reads, extracts, and loads data from comma-separated values (CSV) files or from a database connection. When exporting data, it outputs CSV files. Data Loader offers the following key features: • An easy-to-use wizard interface for interactive use • An alternate command-line interface for automated batch operations (Windows only) • Support for large files with up to 5 million records • Drag-and-drop field mapping • Support for all objects, including custom objects • Can be used to process data in both Salesforce and Database.com • Detailed success and error log files in CSV format • A built-in CSV file viewer • Support for Windows and Mac					
DBM-6	Describe how the system maintains an automated history of all transactions, including, but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update.	X	X		
Response: Within the platform, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include: • Record Modification Fields. All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information. • Login History. You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce. The government can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user's detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary. • Field History Tracking. You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. • Setup Audit Trail. Administrators can also view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to your organization's configuration. This trail can be downloaded into Excel or as a csv file. While the Login History and Setup Audit Trail are available for six months within Salesforce, audit trails can be downloaded and stored locally to meet longer audit log retention requirements. Detailed application logs can be used for forensics investigations by customers. These logs are stored for 12 months and are available for a fee.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-7	Describe how the software database conforms to the Open Database Connectivity Standard (ODBC).	X	X		

Response:

Salesforce uses Oracle DB to power its Databases. Salesforce also uses Postgress and a few other languages but the majority of the Platform runs on Oracle DBs. Salesforce Database is managed inside the Platform and uses the Concept of (Object-for DB Tables | Fields - for DB Columns | Records - For DB Rows) Triggers, APEX Classes and Workflow can be used to run DMLs on Data Saleforce offers multiple APIs that allow you to interact (connect) to Salesforce.

- REST API
- SOAP API
- BULK API
- METADATA API

Full List here : https://help.salesforce.com/articleView?id=integrate_what_is_api.htm&type=5

DBM-8	Describe how the system provides utilities or other tools for administrative users to evaluate data relationships between tables.	X	X		

Response:

The Salesforce platform that BasicGov is built on has an embedded Schema Builder to allow the State to design, visualize and evaluate the data relationships between tables. Schema Builder provides a dynamic environment for viewing and modifying all the objects and relationships in your app. This greatly simplifies the task of designing, implementing, and modifying your data model, or schema.

You can view your existing schema and interactively add new custom objects, custom fields, and relationships, simply by dragging and dropping. Schema Builder automatically implements the changes and saves the layout of your schema any time you move an object. This eliminates the need to click from page to page to find the details of a relationship or to add a new custom field to an object in your schema.

Schema Builder provides details like the field values, required fields, and how objects are related by displaying lookup and master-detail relationships. You can view the fields and relationships for both standard and custom objects.

Schema Builder lets you add the following to your schema:

- Custom objects
- Lookup relationships
- Master-detail relationships
- All custom fields except: Geolocation

DBM-9	Describe how the system prevents corruption or loss of data already entered into the system in the event of failure.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data. Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities unless they are to be retired and destroyed through a secure destruction process. The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.					

Backup and System Recovery Requirements

The system must create backup copies of the software and restore and use those backup copies for the basic protection against system problems and data loss. This requirement refers to all application system files, data files, and database data files. The system must provide a comprehensive and easily manageable backup and recovery process.

The system must have a recovery plan that ensures component failures do not disrupt services. The plan must be completed, implemented, and tested prior to system implementation.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-1	Describe the Backup and System Recovery plan and readiness. Describe the service level agreement on returning the system to service from a backup. Describe the backup retention schedules – daily, weekly, monthly, quarterly, etc.	X	X		
Response: Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data. Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process. The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.					
BKP-2	Describe all needed hardware, software, and tools, and define all roles, responsibilities, processes, and procedures. The system must be sufficiently flexible to integrate with existing DHHS capabilities and accommodate future changes.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: BasicGov is a cloud-based SaaS (software-as-a-service) solution. Our proposed solution is built on the Salesforce Force.com platform and includes all needed infrastructure, which is fully hosted, managed, and maintained by Salesforce. The BasicGov solution only requires a computer that can run a web browser and an Internet connection or a connected mobile device. No other software or hardware is required. Note that Salesforce applications are delivered on-demand over the Internet, so the State will not need to worry about licensing software or setting up and managing hardware platforms. BasicGov products are available on a "per user/subscription" licensing model. Salesforce is a pure multi-tenant, cloud-based web application. Multi-tenancy gives applications elasticity. Force.com applications can automatically scale from one to tens of thousands of users. Processing more than 4 billion transactions each day, Force.com is used for large-scale deployments. Any application that runs on Force.com is automatically architected to seamlessly scale from 1 user to 100,000 users without the customer having to do anything differently. All applications (includes mobile, offline and read-only options) and data running on Force.com are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization's mission-critical applications. Transaction throughput information is published daily on http://trust.salesforce.com/trust/status/. Salesforce routinely processes over 4 billion transactions during normal business days. Of the over 4 billion transactions performed daily on the Salesforce multi-tenant infrastructure, over 50% of these transactions are through the API. In general, we average response times around 250 milliseconds. Since Salesforce is delivered over the web, the number of users will have little effect on user's performances. As a multi-tenant cloud provider, Salesforce puts governance in place to confirm background processes or other activities in the system do not adversely affect the State or other customers' performance.					
BKP-3	Describe the Disaster Recovery Plan. Describe the service level agreement on returning the system back to operational service.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

The service is delivered using a world-class data center infrastructure consisting of a production data center, a full capacity disaster recovery data center plus a separate production-class lab.

Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center.

The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links.

For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center.

Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location. Results of Salesforce's Disaster Recovery tests can be provided to the State upon request.

Under NDA, the State can be provided with Salesforce's complete FedRAMP Authority to Operate (ATO) package, which contains the Salesforce Government Cloud Disaster Recovery Plan as well as the following security assessment documentation:

01 - Salesforce Government Cloud System Security Plan

02 - Salesforce Government Cloud System Security Plan - Tracked Changes

03 - Salesforce Government Cloud Attachment 1 - Control Tailoring Workbook (CTW)

04 - Salesforce Government Cloud Attachment 2 - Control Implementation Summary (CIS)

05 - Salesforce Government Cloud Attachment 3 - PTA and PIA

06 - Salesforce Government Cloud Attachment 4 - E-Authentication

07 - Salesforce Government Cloud Attachment 5 - FIPS 199 Categorization

08 - Salesforce Government Cloud Attachment 6 - User Guide - Customer Configurations

09 - Salesforce Government Cloud Attachment 7 - Hardware, Network, and Software System Inventory

10 - Salesforce Government Cloud Attachment 8 - Customer Responsibilities

11 - Salesforce Government Cloud Rules of Behavior - Ground Rules for Security Success

12 - Salesforce Government Cloud Disaster Recovery Plan

13 - Salesforce Government Cloud Incident Response Plan

14 - Salesforce Government Cloud Configuration Guide

15 - Salesforce Government Cloud Continuous Monitoring Plan

16 - Salesforce Government Cloud Security Assessment Plan

17 - Salesforce Government Cloud Security Assessment Report (SAR)

18 - Salesforce Government Cloud Table 4.1 SAR

19 - Salesforce Government Cloud Test Cases (SRTM)

20 - Salesforce Government Cloud POA&M

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-4	Describe how backups of the system are able to be scheduled without user intervention and without interruption to the system.	X	X		

Response:

Salesforce, and by extension, BasicGov provide multiple ways for our customers to obtain periodic backups of its data. We offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system).

- Direct Export - Data can be exported directly into csv (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users.
- Excel Connector - Salesforce provide an Excel Connector to push and pull data from Excel to Salesforce.com and vice versa.
- Salesforce API - Data can be exported to and from the system though our API at any time or via a number of built in features.
- Salesforce Data Loader - The Salesforce.com Apex Data Loader is a free tool which is used specifically for importing/updating/exporting data in Salesforce.com.
- Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples include: Informatica, Actian, CastIron, Boomi, etc.

BKP-5	Describe how the system provides testing and validation processes for all of the backup requirements listed previously (BKP-1, BKP-2, BKP-3 and BKP-4).	X	X		

Response:

There are several integrity checks performed on the system:

- Input validation on standard fields
- Backups are tested for integrity
- Disaster recovery tests with customer involvement
- Oracle database functionality has built-in integrity checks

In addition to what is described in Req# BKP-4 above, Salesforce has developed additional procedures, processes and plans, including a Pandemic plan.

The Salesforce service is built for high availability at both primary and disaster recovery sites. Each site includes the following:

- Multiple network carriers for customer connectivity
- Multiple ISPs for customer transit and internal replication
- Multiple dedicated connections for DR/BCP
- Redundant routers at entry points
- Redundant firewalls
- Redundant load balancers
- Redundant hubs/switches at VLANs
- Web, Application, API, Cache, Search, Index, Query and Batch servers are load balanced and clustered, with fail-over capabilities
- Database servers are Oracle RAC with 8-node clusters sized to sustain peak load
- Storage has multiple paths for reliability, 4 inter-connects per DBMS server and alternate paths to separate storage directors

Business continuity plans are updated each year, including the list of business processes, recovery time objectives, and key resources. Senior management is included in this process. Business continuity plans are exercised on an annual basis. Action items and lessons learned are tracked from each incident and exercise conducted. Action items are prioritized and tracked until closed.

The Global Business Continuity Policy is available to all employees and is signed off on by Legal and Senior Management.

A global Business Impact Analysis (BIA) has been implemented with over 350 business processes and more than 65 business continuity plans reviewed to identify operational and financial impacts from any sort of unplanned disruption to Salesforce's business operations.

Salesforce manages the BIA application on the Force.com platform which allows the BIA to remain "evergreen". For each business function, the BIA application captures process criticality, possible qualitative and quantitative impacts, critical applications and vendors, locations, and other information that will help identify any recovery risks and/or any recovery gaps where mitigation is needed.

This innovative process provides the ability to automatically update BIA results whenever changes are made to plans, e.g. to processes, tools, or locations, during quarterly plan reviews, thereby beating the industry standard of a yearly update and having an ongoing view into the business risks for Salesforce. The application is also used to generate dashboards and reports to educate Executives on possible risks, and the ability to drill down during incidents or response exercises in order to focus on the possible impact to given business operations.

A key element of the Disaster Recovery plan is Site Switching, which enables the seamless redirection of customer requests from an instance in the primary data center to a replicated instance at a secondary data center. Each instance (for example, NA1 or CS2) contains many servers and other elements to make it run, which is exactly duplicated at the secondary data center. Site Switching minimizes service disruptions when a disaster occurs; it is also useful for minimizing downtime during planned maintenance.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
The Site Reliability (SR) team plans and conducts regular Site Switching exercises. Resulting improvements are identified and implemented within the Disaster Recovery plan. Site-switch exercises have been incorporated into all new instance validations. Each site switching exercise has a similar objective and a consistent standard to validate newly developed recovery scripts and identify any issues that may impact the ability to recover. Prior to each site-switch exercise, the team performs a dry run where each step on the runlist is tested. After a successful dry run, the team performs the site-switch exercise during a weekend of planned downtime.					
BKP-6	If there is a backup failure or downtime, describe the method and timing of communication to DHHS.	X	X		
Response: The Salesforce Services is designed with the concept of continuous improvement and Trust (e.g. Availability, Performance and Security) in the infrastructure. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Salesforce generally does not focus on a specific percentage, as we do not believe our job on availability will ever be "complete". Live and historical statistics on Salesforce system performance are publicly published at: http://trust.salesforce.com/trust/instances. Additionally, please see Req# BKP-4 above for more information.					

Security and Audit Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-1	Describe the security safeguards integrated into their application and how these safeguards address DHHS security. Refer, for example, to DHHS Information Technology (IT) Access Control Standard ((DHHS-IT-2018-001B) for specific requirements: http://dhhs.ne.gov/ITSecurity	X	X		

Response:

Login access to the BasicGov solution is via Username and Password.

Salesforce also offers the following ways to use single sign-on:

- Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. When federated authentication is enabled, Salesforce does not validate a user's password. Instead, Salesforce verifies an assertion in the HTTP POST request, and allows single sign-on if the assertion is true. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.
- Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization.

When you have an external identity provider, and configure single sign-on for your Salesforce organization, Salesforce is then acting as a service provider. You can also enable Salesforce as an identity provider, and use single sign-on to connect to a different service provider. Only the service provider needs to configure single sign-on Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity product.

To enable users to do their job without exposing data that they do not need to see, Salesforce provides a flexible, layered sharing design that allows you to expose different data sets to different sets of users. All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data.

There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security. Details about sharing models and sharing model elements are provided below:

- To specify the objects that users can access, you can assign permission sets and profiles.
- To specify the fields that users can access, you can use field-level security.
- To specify the individual records that users can view and edit, you can set your organization-wide sharing settings, define a role hierarchy, and create sharing rules.

For more information, please refer to the Salesforce Security Guide here: http://sfdc.co/SecurityImplementationGuide.

Salesforce supports multi-factor authentication options and through IP address white listing can enforce region constraints on user access.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-2	The system must comply with Federal, State, and division-specific security requirements including but not limited to: 1. Health Insurance Portability and Accountability Act (HIPAA) of 1996 2. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 3. Nebraska Electronic Signature Statute http://www.nebraskalegislature.gov/laws/statutes.php?statute=86-611 4. Privacy Act of 1974 5. 45 CFR 164 Security standards for PHI Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (http://dhhs.ne.gov/ITSecurity) Due to PHI, DHHS will not give access or demonstrate the current system. Our current data systems include System Automation's License 2000 and the federal government's Aspen Central Office.	X	X		

Response:

Security is a multidimensional business imperative that demands consideration at every level, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum.

In its commitment to provide an on-demand enterprise application that is accessible to all individuals, Salesforce seeks to meet the requirements outlined in the Web Content Accessibility Guidelines (WCAG) 2.0 at Level A.

The Salesforce application incorporates a number of accessibility features that ensure all users have access and can use the application. Many of the features are provided in Accessibility Mode, which can be enabled on an individual user basis. Accessibility Mode can provide a better user experience for users interacting by keyboard only or a screen reader. To help meet our goal of universal design, Salesforce follows the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA to the extent possible.

The Voluntary Product Accessibility Template (VPAT) is a standardized form developed in partnership by the Information Technology Industry Council (ITI) and the U.S. General Services Administration (GSA) to document a product's conformance with key regulations of Section 508 of the Rehabilitation Act. These documents describe how federal agencies can use Salesforce accessibility features.

A third-party vendor has completed an accessibility assessment of Salesforce's core products and has documented their accessibility status using these VPATs.

Copies of our VPATs are available on the Salesforce website at: https://www.salesforce.com/company/legal/508_accessibility.jsp

The VPATs are encompassing of the features and functions of the Salesforce core products and provides an explanation of supporting features with each of the listed 36 CFR 1194 accessibility standards that have been determined to be applicable to this solicitation. If required, Salesforce will make itself available to review the VPAT and features with the State's Accessibility team to determine the requirements and our ability to assure accessibility.

Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties:

Global Audit & Compliance

- ISO 27001
- ISO 27018
- CSA STAR
- SOC 1 Type II (SSAE 16 Report)
- SOC 2 Type II (Trust Principles Report)
- SOC 3 (formerly SysTrust)
- PCI-DSS
- TRUSTe Certified Privacy Seal

Geographical Recognition

- EU Safe Harbor - self-certification through the U.S. Department of Commerce
- FedRAMP (NIST 800-53) - US Government Sector specific
- Japan Privacy Seal - PrivacyMark from the JIPDEC
- TÜV Rheinland Certified Cloud Service - German Certification addressing data protection and data security in conformance with ISO 27001 and the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
See http://content.trust.salesforce.com/trust/en/learn/compliance/ for more details. **HIPAA** Salesforce's customers are responsible for complying with HIPAA's Privacy Rule and Security and the HITECH Act in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. Salesforce can assist customer's with their compliance obligations; for example, by discussing entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI).					
SEC-3	Describe how the system meets the DHHS requirements for unique user ID access. Include: 1. Specification on configuration of the unique user ID. 2. How the unique user ID is assigned and managed. 3. How the unique user ID is used to log system activity. 4. How the system handles the creation of duplicate user ID accounts.	X	X		
Response: The unique ID used for logging into the platform is based on the corporate email address of the individual user. This is determined by the system administration users on creation of individual account. Each user within the platform is also automatically assigned a unique Salesforce ID. 1. The unique user ID must be a unique email address 2. Users will be created by System Administrators within the State Organization. 3. All activity is logged against the Unique user ID, but for usability purposes, activities are listed against the User's 'alias' 4. Duplicate user IDs are not permitted within the platform.					
SEC-4	Describe how the system meets the DHHS standard for administering passwords: 1. Initial Password assignment. 2. Strong Password Requirements. 3. Password reset process. 4. Password expiration policy. 5. Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The platform provides each user in the State's organization with a unique username and password that must be entered each time a user logs in. Administrators can configure several settings to ensure that users' passwords are strong and secure. 1. Initial passwords are created by the user through a double opt-in email process when the account is created. Users must authenticate and create a password that fits within the organization's password policies as well as provide a response to a security question for their first login. 2. Complexity requirements are fully configurable within the platform. The State will set password history, length, and complexity requirements. You can also specify what to do when a user forgets the password. Options for password complexity include the following: a. No restriction—Has no requirements and is the least secure option. b. Must include alpha and numeric characters—The default setting. Requires at least one alphabetic character and one number. c. Must include alpha, numeric, and special characters—Requires at least one alphabetic character, one number, and one of the following characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. d. Must include numbers and uppercase and lowercase letters—Requires at least one number, one uppercase letter, and one lowercase letter. e. Must include numbers, uppercase and lowercase letters, and special characters—Requires at least one number, one uppercase letter, one lowercase letter, and one of the following characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. f. Must include 3 of the following: numbers, uppercase letters, lowercase letters, special characters—Requires at least three of the following options: one number, one uppercase letter, one lowercase letter, and one special character (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~) 3. Passwords may be reset by the Administrator in the back-office solution, or by an individual user by clicking on "Forgot Password" on the login page. In the latter case, the user must successfully answer their designated security question to reset the password. 4. The default expiration dates for passwords in the platform is 90 days although this is fully configurable. 5. The number of login failures allowed for a user before the user is locked out is fully configurable in the platform.					
SEC-5	Describe how the system meets the requirements for unique system administration access. Include: 1. Specification on configuration of the unique system administration ID, (approximately 30 with ability to access and manage the applications across all license types). 2. How the unique system administration ID is assigned and managed. 3. How the unique system administration ID is used to log system activity.	X	X		
Response: System administration access is controlled by the user profile settings in the platform. By default, the System Administrator profile has full access to manage the applications across all license types however it is also possible to set up other system administrator type profiles who would have management rights only over specific areas of the application. Access to the platform is managed in the same way as other user access. The key differentiator is the permissions provided based on the User's profile.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-6	Describe how the system meets the requirements for unique database administration access. Include: 1. Specification on configuration of the unique database administration ID. 2. How the unique database administration ID is assigned and managed. 3. How the unique database administration ID is used to log system activity.	X	X		
Response: Salesforce provides strong audit capabilities. Each user has a profile & a role. Profiles control the activities /functionalities that a user has access to. Salesforce offers "System Administrator" profile that has complete rights over the system. This profile can be assigned to State defined users who are required to carry out admin activities. Complete log of who/ when/ what/ from where is available within Salesforce for all the profiles. Since Salesforce is PaaS (Platform as a Service), access to underlying database is not available.					
SEC-7	Describe how the system supports the use of multi-factor authentication.	X	X		
Response: Multi-factor authentication can be managed with the use of Salesforce Authenticator along with the BasicGov solution. Salesforce Authenticator is a smart, simple, two-factor authentication solution that increases the security of a deployment while driving a better end-user experience. Like soft tokens, Salesforce Authenticator leverages a user's mobile device, making it easy and inexpensive to deploy and manage. However, Salesforce Authenticator advances beyond the limitations of traditional two-factor techniques by using un-phishable, out-of-band approvals. When an action needs to be authenticated, the user is sent a push notification. The user sees contextual information about the authentication and has the option to approve the request or deny it. And since this all happens in a secured, secondary channel, not only is usability improved, but so is the security.					
SEC-8	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

The Salesforce platform that BasicGov is built on has comprehensive privacy and security assessments and certifications performed by multiple third parties:

Global Audit & Compliance

- ISO 27001
- ISO 27018
- CSA STAR
- SOC 1 Type II (SSAE 16 Report)
- SOC 2 Type II (Trust Principles Report)
- SOC 3 (formerly SysTrust)
- PCI-DSS
- TRUSTe Certified Privacy Seal

Geographical Recognition

- EU Safe Harbor - self-certification through the U.S. Department of Commerce
- FedRAMP (NIST 800-53) - US Government Sector specific
- Japan Privacy Seal - PrivacyMark from the JIPDEC
- TÜV Rheinland Certified Cloud Service - German Certification addressing data protection and data security in conformance with ISO 27001 and the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)

See http://content.trust.salesforce.com/trust/en/learn/compliance/ for more details. Salesforce regularly performs self-vulnerability assessments using various tools and techniques, including tools such as Qualys. In addition, Salesforce uses external service providers to perform an application vulnerability assessment after each major release (three times annually) and network vulnerability assessments quarterly. Executive summary reports can be shared upon request and under NDA.

Scans are done against applications as well as network type vulnerabilities, such as discovering browser exploits or similar application issues.

Salesforce runs antivirus software on the production systems that store, transmit or process customer information. The Anti-virus scans host filesystems (not customer data). The antivirus software checks for virus definition updates daily. Other controls are also used to address malware such as hardening the Operating System of our servers, firewall configuration to ensure only required ports are open and all others denied and use of intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real time through a security monitoring system.

The application only accepts http and https traffic, but Salesforce does not restrict the file types users can upload. Salesforce does not modify or clean any customer data; the system stores the information provided in an encoded format within the database. It is recommended that customers run updated antivirus and antimalware solutions to help mitigate these threats. The production system receives inbound mail as part of the workflow functionality, but this does not pose any threat to our network, application, or users. No code in the email can be executed or transferred, eliminating the malicious software risk. Email sent from the Salesforce system is not currently scanned for viruses.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-9	Describe how the system provides the ability to maintain a directory of all personnel who currently use or access the system.	X	X		
Response: A directory of all personnel who currently use or access the system is a standard function of the platform's user management capabilities. Administrators can perform tasks such as: • Create and edit users • Reset passwords • Create Google Apps accounts • Grant permissions • Create and manage other types of users • Create custom fields • Set custom links • Run reports on users • Delegate user administration tasks to other users					
SEC-10	The State of Nebraska requires authentication and authorization of users through an enterprise directory known as the Nebraska Directory Services (NDS) to access web-based applications. Describe how the system will integrate NDS authentication. Refer to the Nebraska Information Technology Commission Security Architecture – Authentication and Authorization – Identity and Access Management Standard for State Government Agencies (8-303) for specific requirements: https://nitc.nebraska.gov/standards/8-303.pdf	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via a TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application. In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce. Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally, your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce. Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.				
SEC-11	Describe how the system provides rule-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database system). Describe the security administration functions integrated into the system that manage role-based access to system functions, features, and data. Include a description of: 1. How and where the system stores security attributes or roles (e.g., LDAP attributes, database tables, files). 2. The interface between the LDAP and the application, if roles are assigned in an LDAP directory. 3. How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each). 4. How groups are defined and how roles and security are applied to each group. 5. How access limits are applied to screens and data on screens by role or group. 6. How users are created and assigned to one or more roles or groups. 7. How role and group creation and assignment activity is logged.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The platform has robust security and data privacy features modeled around the concept of user profiles, roles and permission sets. Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization. When you have an external identity provider and configure single sign-on for your Salesforce organization, Salesforce is then acting as a service provider. You can also enable Salesforce as an identity provider and use single sign-on to connect to a different service provider. Only the service provider needs to configure single sign-on Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity product. To enable users to do their job without exposing data that they do not need to see, Salesforce provides a flexible, layered sharing design that allows you to expose different data sets to different sets of users. All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. A profile contains the settings and permissions that control what users with that profile can do within Salesforce, the partner portal, and the Customer Portal. Profiles control: • Standard and custom apps the user can view (depending on user license) • Service providers the user can access • Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) • Administrative and general permissions the user has for managing the organization and apps within it • Object permissions the user is granted to create, read, edit, and delete records • Page layouts a user sees • Field-level security access that the user has to view and edit specific fields • Record types are available to the user • Desktop clients users can access and related options • Hours during which and IP addresses from which the user can log in • Apex classes a user can execute • Visualforce pages a user can access				
SEC-12	The system must automatically disconnect based upon inactivity, as required by DHHS Security Policies and Standards. Describe how the feature is administered and what effect disconnect has on any activity or transaction in process at the time of disconnection. Refer to DHHS Securing Hardware and Software Standard (DHHS-IT-2018-001A) for specific requirements: http://dhhs.ne.gov/ITSecurity	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The platform has configurable functionality to automatically log a user off the system after a pre-defined inactivity period. While the default disconnect time is 2 hours, it is set in the system administration function in accordance with the organization's policies.					
SEC-13	The system must protect confidential and highly restricted data from unauthorized access during transmission. Describe transmission safeguards that are integrated into the proposed system to protect data during transmission, including any encryption technology. Refer to DHHS Information Technology (IT) Security Policy (DHHS-IT-2018-001) for specific requirements: http://dhhs.ne.gov/ITSecurity	X	X		
Response: The Salesforce platform that BasicGov is built on utilizes some of the most advanced technology for Internet security available today. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization. One of the core features of a multi-tenant platform is the use of a single pool of computing resources to service the needs of many different customers. Salesforce protects your organization's data from all other customer organizations by using a unique organization identifier, which is associated with each user's session. Once you log in to your organization, your subsequent requests are associated with your organization, using this identifier. In addition, Salesforce is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders. Salesforce requires that cipher suites used for outbound calls meet security standards. Check your servers' cipher suite lists and ensure that they support the advanced encryption standard (AES) with 128-bit (AES128) or 256-bit (AES256) stream keys. Otherwise, custom code that relies on outbound calls to the HTTPS server fails				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-14	The system must provide auditing functions for all data fields, including but not limited to: 1. The user ID of the person who made the change. 2. The date and time of the change. 3. The physical, software/hardware and/or network location of the person while making the change. 4. The information that was changed. 5. The outcome of the event. 6. The data before and after it was changed, and which screens were accessed and used. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: http://dhhs.ne.gov/ITSecurity	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include: • Record Modification Fields. All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information. • Login History. You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce. The government can also track the geographic location of the IP addresses of your logins in your personal settings. You can track the geographic location of the login IP addresses for any of your users in the user's detail page. To get more detailed geographic information, such as city and postal code, you can download the login history. Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary. • Field History Tracking. You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. In addition to Salesforce's core auditing capabilities, Salesforce offers Event Monitoring as an additional license option. The the State can use event monitoring to discover how often and at what times your users are logging in to and out of your organization. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. Not only can the the State now better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put the the State at risk. In addition, the the State can also determine if an employee is unnecessarily downloading sensitive customer/citizen information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available. Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Force.com SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind: • Log data is read-only. You can't insert, update, or delete log data • Use the EventType field to determine which files were generated for your organization • LogDate tracks usage activity for a 24-hour period, from 12:00 a.m. to 11:59 p.m. UTC time • An event generates log data in real time. However, log files are generated the day after an event takes place, during nonpeak hours. Therefore, log file data is unavailable for at least one day after an event • CreatedDate tracks when the log file was generated • Log files, represented by the EventType field, are only generated if there is at least one event of that type for the day. If no events took place, the file won't be generated for that day • Log files are available based on CreatedDate for the last 30 days when organizations purchase User Event Monitoring or one day for Developer Edition organizations • All event monitoring logs are exposed to the API through the EventLogFile object, however there is no access through the user interface				
SEC-15	The system must provide auditing functions for confidential and highly restricted data that is accessed and viewed, regardless of whether the data was changed. Describe the auditing functions which must include but not be limited to:	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
	1. The user ID of the person who viewed the data. 2. The date and time of the viewed data. 3. The physical, software/hardware and/or network location of the person viewing the data. 4. The information that was viewed. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: http://dhhs.ne.gov/ITSecurity				
Response: Please refer to the response to SEC-14 above.					
SEC-16	If the system has the ability to override edits, describe how the system audits all overridden edits and identifies information including, but not limited to, the login ID, date, and time.	X	X		
Response: The platform allows developers and administrators to control access to data at many different levels. You can control access at the object-level, the record-level, and at the field-level. Object-level security within the Salesforce.com environment is referred to as Create-Read-Update-Delete (CRUD) access. CRUD settings are applied at the profile level and can be used to restrict the actions that users can take on each type of standard and custom object. Field-level security (FLS) is configured similarly to CRUD but allows administrators to define the profiles that can see and write to most fields of standard and custom objects. Authorized users can override edits, and auditing function follows as described in previous response to Req#SEC-15 above.				
SEC-17	Describe how the system produces daily audit trail reports and allows inquiries, showing updates applied to the data.	X	X		
Response: Please refer to the response to SEC-14 above.					
SEC-18	Describe how the system provides an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: When Records are deleted from the System they are stored in the Recycle BIN to be able to easy restore the Records if need be. Deleting the Records from Recycle BIN permanently removes Records from Salesforce. The Recycle BIN can contain 25 Times your MB Storage capacity. For example, an org with a storage allocation of 2,000MB (2GB) can have 50,000 records in the Recycle Bin: 25 x 2,000 = 50,000 records. Deleted Records can stay in the Recycle BIN for 15 days before they are permanently deleted. System Debug Logs are retained for 24 Hours Monitoring Debug Logs are retained for 7 Days Debug Logs can only be 20 MB you can reduce the size by removing the older Log Lines BasicGov offers a Batch - Delete Rule in the Dynamic Rules Engine (DRE) to delete Records based on predefined criteria. Additionally, Salesforce offers a Mechanism to run Batch Processes (Batch Classes) that runs in the background and that can be execute for records that match predefined criteria and execute a DML - Delete accordingly. Example: Delete All Debug Log Records Daily at the end of the day or Delete Records that match certain criteria.					
SEC-19	Describe how the system supports encryption of data at rest or an equivalent alternative protection mechanism. Describe the proposed encryption of data. If data is not encrypted, describe in detail compensating controls.	X	X		
Response: Encryption of data at rest is supported by the Salesforce Shield optional module. Shield Platform Encryption gives data a layer of security while preserving critical platform functionality. It enables the State to encrypt sensitive data at rest, and not just when transmitted over a network, so the State can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data. Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system, so it's protected even when other lines of defense have been compromised. Shield Platform Encryption lets the State encrypt a wide variety of standard fields and custom fields. It can also encrypt files and attachments stored in Salesforce, Salesforce search indexes, among others. Data encryption key material is never saved or shared across orgs. The State can choose to have the platform generate key material for them or upload it's own key material. By default, the Shield Key Management Service derives data encryption keys on demand from a master secret and the org-specific key material, and stores that derived data encryption key in an encrypted key cache. The State can also opt out of key derivation on a key-by-key basis, or store the final data encryption key outside of the platform and have the Cache-Only Key Service fetch it on demand from a key service that the State controls. No matter how keys are managed, Shield Platform Encryption secures the State's key material at every stage of the encryption process					
SEC-20	Describe how the system adheres to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The platform offers multiple layers of Security that make it robust in many ways, starting from authentication, data visibility, different mechanism for Data Encryption and also Code Specific security measure that prevent Phishing and Malware, External URL redirects, SQL Inject, etc. The Platform utilizes advanced Technology Internet Security. When you access the application using a Salesforce-supported browser, Transport Layer Security (TLS) technology protects your information using both server authentication and Classic Encryption, ensuring that your data is safe, secure, and available only to registered users in your organization. Administrator can use a utility called "Security Health Check" to identify potential vulnerabilities in security settings.					
SEC-21	Describe how the system is configurable to prevent corruption or loss of data already entered into the system in the event of failure.	X	X		
Response: Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned at an archive data center. Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across data centers). Backups are retained for 90 days. Backups never physically leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process. For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4-hour recovery point objective (RPO) and 12-hour recovery time objective (RTO).					
SEC-22	Describe how the system, upon access, displays a message banner indicating that this application is only to be accessed by those individuals who are authorized to use the system.	X	X		
Response: Message banners may be configured in the platform to be displayed on the login page or on any page once the user logs in tot the system.					
SEC-23	Describe how the system, prior to access of any confidential or highly restricted data, displays a configurable warning or login banner (e.g. "The system must only be accessed by authorized users"). In the event that the system does not support pre-login capabilities, describe how the system displays the banner immediately following authorization.	X	X		
Response: The State can configure a warning on the login page to be displayed to all users prior to logging into the system.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-24	Describe how the system recognizes confidential and highly restricted data in screens, reports, and views (i.e. PHI and SSN), and restricts distribution and access based upon system security settings and roles. Include warnings on printed and viewed reports.	X	X		
Response: The platform will allow the State to designate some data fields as encrypted fields thereby masking the data in those fields to all users. Only users with the permission "View Encrypted Data" can see data in encrypted custom text fields. The security settings of the encrypted are maintained through the User Profile of the user viewing the field and persist across all usage, including reporting, printing, and exporting of data.					
SEC-25	The system or Contractor must alert DHHS of potential violations of security and privacy safeguards. Incidents that involve or could potentially involve confidential or highly restricted data must be reported immediately as defined in DHHS Policy DHHS-2018-IT-001E DHHS IT Incident Management Standard.	X	X		
Response: In addition to the Security Health Check functionality, Salesforce provides access to trust.saleforce.com. Among other things, this Site provides information about Recent Security Advisories in which Security Concerns are addressed (https://trust.salesforce.com/en/security/security-advisories/) and a way to contact Salesforce with any possible Security Concerns. Salesforce keeps a very transparent model in which the Status on the Platform and Incident are reported. Also includes best Security practices for Developers to prevent vulnerabilities.					
SEC-26	Describe how the system provides the capability to monitor events on the information system, detects attacks, and provides identification of unauthorized use of the system.	X	X		
Response: Salesforce offers Event Monitoring as an additional license option. The State can use event monitoring to discover how often and at what times your users are logging in to and out of your organization. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. Not only can the State now better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put the State at risk. In addition, The State can also determine if an employee is unnecessarily downloading sensitive customer/citizen information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available. Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Force.com SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily.					
SEC-27	The system must provide a process for archiving or destroying data and sanitizing storage media in conformance with DHHS and Division data governance policies and subject to applicable HIPAA, and federal (e.g., Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), and State laws.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Salesforce Provide "Data Storage" view that allows you to see what Objects are consuming most space and then you can use a tool such as Saleforce Data Export, SFDC Data Loader or other Third Party Tools to Backup Data such as Gearset, Informatica, Boomi, DBAmp to mention some, that allow you to export and store Data in External Databases and free up Salesforce from Historical and unnecessary Data. Salesforce Out of the Box Data Export allows you to generate BackUp Files on weekly or monthly basis and export as CSV Files, this Data can be then loaded into an External Database and then remove from SFDC. Paid Third Party Tools offers more sophisticated ways to handle Data Archiving and Purging.					
SEC-28	Describe how the system provides the capability to identify and report on unauthorized attempts to access information in the system, based on user-defined criteria.	X	X		
Response: Through event monitoring in Salesforce Shield, the system will identify and report on unauthorized attempts to access information in the system. Transaction security policies monitor events, which are categories of user activity built on objects in the SOAP, REST, and Bulk APIs. When you build your policy using Condition Builder, you choose which fields on these objects you want to monitor for customer activity. Because your policy's actions are conditional to the fields that users interact with, these fields are called conditions. When you create a policy, you choose the conditions you want your policy to monitor. The conditions available in Condition Builder are a subset of all the event objects fields and vary based on the objects. If you create an Apex-based policy, you can use any of the event object's fields. For example, Records isn't available as a Condition Builder condition for the ReportEvent event object.					
SEC-29	Describe how the system has defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes.	X	X		
Response: Salesforce uses Oracle DB to power its Databases. Salesforce also uses Postgress and a few other languages but the majority of the Platform runs on Oracle DBs. Salesforce Database is managed inside the Platform and uses the Concept of (Object-for DB Tables | Fields - for DB Columns | Records - For DB Rows) Triggers, APEX Classes and Workflow can be used to run DMLs on Data. Saleforce offers multiple APIs that allow you to interact (connect) to Salesforce. • REST API • SOAP API • BULK API • METADATA API Full List here : https://help.salesforce.com/articleView?id=integrate_what_is_api.htm&type=5					
SEC-30	The system must be able to export audit logs that can be used with a third party Log Management & Analysis tool. Describe how the system exports logs in such a manner as to allow correlation based on time (e.g. Universal Time Coordinate (UTC) synchronization.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Audit logs can be exported through standard reporting and data export functions in the platform or through standard API's built into the platform.					
SEC-31	Describe how the system supports removal of a user's privileges without deleting the user from the system to ensure a history of user's identity and actions.	X	X		
Response: A user may either be de-activated or frozen in the platform. Both result in the user's privileges being removed while still maintaining the history of the user's identity and actions.					

Data Conversion Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DAC-1	Describe the process for converting all historical data from the Department's existing systems, spreadsheets, and other supporting applications that are required for ongoing operations of the system and the historical reporting needs of the department. System Automation's License 2000 (Oracle) currently contains approximately 655 tables and 50 million records. DHHS also has approximately twelve (12) Access/Excel databases. Some information in these databases does not tie to license information in L2K. DHHS also uses the federal government's Aspen Central Office to import licensure data on a daily basis.	X	X		

Response:

We will develop a template that will be used for Dataloads to Salesforce. The data extracted from State's systems/ files will be transformed into appropriate format before the load. We anticipate following steps in the data migration process:

- Data Migration Planning
- Data Extraction
- Data Transformation
- Data Load Sequencing
- Data Load & Extract (for reference fixing)
- Data Load

The data load will be performed in following cycles:

- Test Data Load (partial load for Testing purposes)
- Mock Data Load (full load before Production load to uncover any potential migration issues)
- Production Data Load (before the go-live)

The State will be responsible for extracting and converting data and providing it in a compatible format for data migration.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DAC-2	Describe the data conversion plan which includes data element mapping crosswalks, data cleansing, data synchronization for initial and interim conversion activities leading up to the final data conversion, and frequency of interim conversion events and final conversion execution. Contractor will be responsible for all data standardization and cleansing. It is acceptable to migrate data and go live with license applications in incremental steps. For individual licensees, SSN is included in L2K. There is also an identifier called “Person ID” in L2K. For establishments in L2K, there are unique license numbers by license type, and unique applicant numbers. In ACO, establishments have unique license numbers by license type.	X	X		
Response: Kindly refer response to DAC-1.					

Production, Test and Training Requirements

DHHS requires three separate environments (Production, Test, and Training) in order to operate and maintain the new software on an ongoing basis:

Test Environment – A test environment is required that mirrors the live production environment, including hardware and software. This test environment will be used to test application changes before deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

Training Environment – A training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique data for use in training and conduct training without interference with the test or production environments. This environment will have occasional use.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	© 3rd Party
PTT-1	Describe how the system supports several environments, i.e., production environment, test environment, and training environment.	X	X		
Response: Salesforce provides several Sandboxes for development and testing purposes before the application is made available to end-users. We anticipate use of following type of Sandboxes or Environments: 1. Development Environment / Sandbox 2. Systems & Integration Testing Environment / Sandbox 3. Training & User Acceptance Testing Environment/ Sandbox 4. Hot-fix Environment / Sandbox (State will need after Go-live) 5. Pre-Production Regression Testing Environment / Sandbox (State will need this after go-live) Spinning up a new environment from Salesforce is pretty easy and can be done with few clicks. It also provides capability to clone environments. Some specific data can be masked while cloning/ copying the environments (like email addresses), so that testing the data does not result in accidental relay of emails to real end-users. Other confidential data can also be masked or transformed.					
PTT-2	Describe how the system supports non-production environments such as testing and training environments. Training environment must contain de-identified data and not include confidential or highly restricted data.	X	X		
Response: Please refer to response on PTT-1.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	© 3rd Party
PTT-3	Describe how the system provides the ability to refresh any testing or training environment at the request of DHHS. Describe the refresh process and whether the refresh process can be completed using DHHS resources, or whether the process requires professional services from the Contractor.	X	X		

Response:

An environment/ sandbox can be refreshed with a matter of clicks in Salesforce. Following types of sandboxes are available in Salesforce:

- Developer - Special configuration-only sandboxes intended for use developers
- Developer Pro - Includes a copy all of your production organization's reports, dashboards, price books, products, apps, and customizations under Setup, but exclude all of your organization's standard and custom object records, documents, and attachments
- Partial Data - Includes all of your organization's metadata and add a selected amount of your production organization's data that you define using a sandbox template
- Full Copy - Includes a copy your entire production organization and all data, including standard and custom object records, documents, and attachments

Some of the best practices for managing these environments are:

- Proper Planning • Determine environment plan at start of project • Map out the required environments (Dev, UAT, Training, etc) at the start of a project and a line up refresh timeframes accordingly • Determine which environments will require data to be migrated manually and plan time to create sample data sets and load events • For example, environments using Developer Pro sandboxes for events such as unit testing or training events • Build time into your plan for deploying configuration between environments
- Determine "sandbox only" users • Some users may only be needed in sandbox environments (for example, developers) • Create these users in your production instance, deactivate them in prod, then reactivate them in the appropriate sandbox after the copy is made • Similarly, some users may need different permissions in a sandbox. Plan to change these users profiles after the sandbox copy is made
- Determine data obfuscation needs and procedures to modify • Modify contact email addresses manually after the sandbox copy is made to ensure real contacts do not get emails during testing efforts • Modify any other sensitive data that should not be shown to developers (for example) like SSN's, Account #'s, etc. may need to be modified manually or through data loader as well
- Document your sandbox refresh procedures for reuse across multiple support personnel • Document the entire environment, along with sandbox names and uses • Document the procedures required after a sandbox refresh is completed – ie, do users need to be enabled in various environments, does test or training sample data need to be migrated to environments?
- Appoint a release and/or environment manager • This individual should oversee all environment plans, decisions, and activities

PTT-4	Describe the test procedures for any changes to the system. Describe user test planning including unit testing, end-to-end testing, stress testing, and readiness testing prior to "go live" date.	X	X		

Response:

Salesforce Apex Unit Testing facilitates the development of robust, error-free code, Apex supports the creation and execution of unit tests. Unit tests are class methods that verify whether a particular piece of code is working properly. Salesforce does not allow any release to Production unless 75% of code is covered using Unit Testing.

Once Sprint build is complete, we plan to do System Testing. System Testing is validating whether all functional requirements/ user stories have been built properly or not. We track the testing progress using various tools (e.g. Jira) and ensure all defects are closed prior to progressing the application to higher environment.

User Acceptance Testing is initiated after full Systems & Integration Testing is completed. Here, we facilitate power users/ functional champs from State to test the System thoroughly.

As Salesforce is hosted PaaS, usually - load testing / endurance testing/ performance testing is usually not required unless the application has been heavily customized. In case, State sees this as a requirement, we can work with State on meeting this requirement.

Salesforce also supports Test Automation (through 3rd party) in case State sees its application as useful.

Cloud SynApps QA lead will work with the State to document a testing strategy and plan that defines the approach and explains the requirements and scope of the test, entry and exit criteria, resources, and key dates. The plan will be signed off prior to the start of the test execution phase.

As part of our implementation plan, the table below outlines the various testing phases and the respective environments where testing is conducted.

Testing Type	Testing Process	Testing Roles & Responsibilities	Testing Environment
Unit Test	Tests each individual unit of the application. The test execution is performed in the later part of the build stage after the application components are coded.	Cloud SynApps Developers	DEV, SIT
System Integration Testing	An end-to-end test of the business requirements across all applications and platforms.	Cloud SynApps QA Lead (support from State's Business Analyst)	QA, UAT
User Acceptance Testing	An end-to-end test of the business requirements across all applications and platforms.	Cloud SynApps QA Lead State's Business Users	UAT
Migration Testing	A mock deployment to verify that all components of the system are collated and can be correctly deployed to the production environment in the time required, and that the system is correctly installed and configured.	Cloud SynApps Developers (support from State's Business Analyst)	SIT, PreProd
Regression Testing	Regression testing ensures that when changes are introduced to a system (as a result of bug fixes or enhancements) they do not adversely affect the functionality of the system.	Cloud SynApps Developers (support from State's Business Analyst)	PreProd

We can work with the State to identify its additional needs for the performance tests during the project implementation and determine if it needs Installation Verification Test, Defect Test, Load Test, Stress Test, etc.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	© 3rd Party
PTT-5	Describe how the system allows changes to be tested before implementation in the production database. Examples include changing licensure requirements, license type name changes, and scripts to replace data.	X	X		
Response: Please refer to PTT-1 response.					

Interfaces/Imports/Exports Requirements

The system is required to be able to interface with other computer systems as necessary.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
INT-1	Describe the automated approach to managing interfaces. HL7 standards are available at www.hl7.org	X		X	
Response: Salesforce provides highly flexible options to integrate it with any other 3rd party applications. It supports both REST and SOAP API. With some customizations, Salesforce can meet HL7 standards for interfaces.					
INT-2	Describe how the system interfaces secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.	X	X		
Response: The platform provides a strong Security Model that relies on Object, Field and Data Permissions based on User Profiles. This means that the CRUD (Create Read Update Delete) model is fully implemented at the Object and Field level. Visibility to Fields can also be restricted at the User Interface Level, for example fields that are visible to a Inspections Manager, are not visible to an Inspector. Additionally, it follows the concept of Sharing Only Records that users are granted to see, which mean it has a model to control Data Visibility using Private, Read Only and Read Write privileges. The platform also offers other mechanism to share Data base on a Role Hierarchy, Sharing Rules with predefined criteria and Manual Sharing Records. On top of the Data Model describe above, Salesforce offers Data Encryption for sensitive Data.					
INT-3	Describe how the system has the capability to notify system administrators/ system support staff if an interface is not available for any reason.	X	X		
Response: Salesforce automatically generates exceptions in case of any Integration failures. Additionally, custom exception handling mechanism can also be built within Salesforce. For any reason, if interface is not available, Salesforce will generate an exception notification and the same can be sent automatically by an email to system administrator.					
INT-4	Describe how the system provides necessary application program interfaces and/or web services to allow DHHS to create interfaces to and from the system. Exact number of imports/exports required. DHHS anticipates disciplinary databanks, compacts, schools, exam companies, and employers may interact with the system.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Salesforce provides support for both SOAP/ REST API (application programmable interface) calls. It provides Enterprise & Partner WSDLs that can be used to read/ edit/create/delete data in Salesforce. Salesforce also provides an option to build custom webservices that can be called by any 3rd party system. Such systems have to be whitelisted in Salesforce in order to allow this integration call.					
INT-5	Describe how the system supports data exchanges between components in real time so that data is always synchronous across the entire system, including any third-party components.	X	X		
Response: Salesforce provides real-time integration capabilities using SOAP and REST APIs. There is no need to have temporary data stores or placeholder to store data for any transformations. Salesforce also works seamlessly with any middleware solution.					
INT-6	Describe how the system has the ability to expand data access to additional systems that are consistent with current data standards.	X	X		
Response: Salesforce provides feature of “Connected App”. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as Security Assertion Markup Language (SAML), OAuth, and OpenID Connect. Connected apps use these protocols to authorize, authenticate, and provide single sign-on (SSO) for external apps. The external apps that are integrated with Salesforce can run on the customer success platform, other platforms, devices, or SaaS subscriptions. By capturing metadata about an external app, a connected app tells Salesforce which protocol—SAML, OAuth, and OpenID Connect—the external app uses, and where the external app runs. Salesforce can then grant the external app access to its data, and attach policies that define access restrictions, such as when the app’s access expires. Salesforce can also audit connected app usage.					
INT-7	Describe how the system conducts end-to-end testing with interface partners, both external and internal, to ensure requirements are met.	X		X	
Response: While writing Apex Unit Tests for checking Integrations, Salesforce provides “WebServiceMock” interface , “doInvoke” method and “Test.setMock” method to fake response in a test method. The interface enables sending fake response when testing web service callouts of a class auto-generated from WSDL. Also, tools like “SOAPUI” can be leveraged to send a test request to Salesforce and check the response. Once the system has been built, end-to-end Integration Testing will be done to test the Interfaces.					

System Performance Requirements

This section describes requirements related to the systems' on-line performance, response times, and sizing from a system architecture standpoint.

NOTE: If your system has specific high availability or redundancy requirements, the requirements must be defined below (see PER-5).

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-1	Describe the system performance functionality and monitoring tools.	X	X		

Response:

Daily service availability data is posted on http://trust.salesforce.com. Salesforce's multi-tenant cloud service provides redundant data protection, advanced facilities protection, and data recovery plan.

In addition to the Salesforce Trust site (http://trust.salesforce.com/trust/status) to monitor uptime and performance, the State will also have access to a System Overview, which will help you monitor performance and usage of your own Salesforce org. This overview includes:

- Schema. # and % of custom objects and data storage
- API Usage. # and % of requests in the last 24 hours
- Business Logic. # and % of Rules, Apex triggers and classes, as well as % of code used

License Usage

- User Interface. # and % of custom apps, sites, flows, custom tabs and pages
- Portal Usage

The above list is of all the possible metrics that you may have in your system overview.

Trust.salesforce.com

Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you will find:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance
- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

The Trust site includes an API that the State can use to directly integrate Salesforce availability information into existing monitoring tools or processes. For example, the State can retrieve the status of a given instance, details on any active availability or performance incidents, transaction performance data, and the upcoming planned maintenance schedule.

Details on all available API endpoints can be found here: http://content.trust.salesforce.com/trust/en/learn/trust-api/ and include:

- Instances. http://content.trust.salesforce.com/trust/en/learn/trust-api/get-instances/
- Instances/:instanceName. http://content.trust.salesforce.com/trust/en/learn/trust-api/get--instances-instancename/
- Calendar. http://content.trust.salesforce.com/trust/en/learn/trust-api/get-calendar/
- Transactions. http://content.trust.salesforce.com/trust/en/learn/trust-api/get-transactions/
- Incidents. http://content.trust.salesforce.com/trust/en/learn/trust-api/get-incidents/
- General Messages. http://content.trust.salesforce.com/trust/en/learn/trust-api/get-general-messages/

Health Check

Health Check lets the State understand and proactively remediate your Salesforce org's security risks and vulnerabilities from a single page.

At a glance, the the State can see and fix security risks for your org in your Session Settings, Password Policies, and Network Access settings. A health check dashboard shows how well your org measures against the Salesforce-recommended baseline.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
The Salesforce Baseline standard contains recommended values for the Session Settings, Password Policies, and Network Access setting groups. If you change all of a group's settings to be less restrictive than what is in the Salesforce Baseline standard, your health check score decreases. The dashboard shows high and medium risk settings and how they compare against the standard. To remediate a risk, click the edit link next to the setting. All of your settings that meet the standard are listed at the bottom. For example, suppose that you changed your password minimum length from 8 (the default value) to 5, and changed other Password Policies settings to be less restrictive. These changes make your users' passwords more vulnerable to guessing and other brute force attacks. As a result, your overall score decreases, and the settings are listed as risks.					
PER-2	Describe the minimum response times for the following functions, even at peak load. For example, expected response time will be within two (2) seconds 95% of the time, and under five (5) seconds for 100% of the time. 1. Record Search Time 2. Record Retrieval Time 3. Transaction Response Time 4. Print Initiation Time 5. Subsequent Page Display Response Time 6. Document Availability Note: These response times do not include network latency, which will be measured and reported by DHHS.	X	X		
Response: 1. Record Search Time - 2 seconds 95% 2. Record Retrieval Time - 2 seconds 95% 3. Transaction Response Time - Depends on what transaction we are referring to but I would say - 2 seconds 95% 4. Print Initiation Time 2 seconds 95% 5. Subsequent Page Display Response Time 2 seconds 95% 6. Document Availability 2 seconds 95%					
PER-3	Describe how the system captures system downtimes, along with the causes of the downtimes where applicable. Describe the method and timing of communication to DHHS on downtimes.	X	X		
Response: Daily service availability data is posted on http://trust.salesforce.com. Salesforce's multi-tenant cloud service provides redundant data protection, advanced facilities protection, and data recovery plan.					
PER-4	Describe how the system supports concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The Salesforce that BasicGov is built on has a heavily instrumented application, which is fed a substantial number of performance metrics into a service delivery data warehouse (DW). This output then drives how Salesforce decides to address capacity changes—the answer is not always "add hardware"—and refactoring parts of the application, using appliances, etc., are often the most appropriate solutions to handle changes in capacity. In general terms, Salesforce has shifted scalability from vertical to horizontal techniques within the infrastructure to increase service capacity. Horizontal scalability allows Salesforce to increase capacity if we believe we are getting near the limit of vertical scalability. The current system is composed of multiple instances for Europe, North America, and Asia Pacific.					
PER-5	Describe how the system is available online 24 hours a day and 7 days a week. Describe any known timeframes where the system will be unavailable for use.	X	X		
Response: Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Salesforce generally does not focus on a specific percentage, as we do not believe our job on availability will ever be "complete". Live and historical statistics on Salesforce system performance are publicly published at: http://trust.salesforce.com/trust/instances.					
PER-6	Describe how the system provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

Overall system monitoring is provided by a variety of tools. All monitoring alerts are aggregated and monitored by the Site Reliability (SR) team. Alerts such as configuration changes from network devices, server state changes, and other events can be correlated to indicate root cause. The dynamic model capability also allows the customization of the monitoring tool to mimic Salesforce Service's hardware/software configuration, so that custom symptoms and problems can be rolled up into the correlation engine.

Salesforce has built extensive monitoring and instrumentation into the application itself, so that the application can accurately report its health and performance to the systems engineers, network operations staff, QA personnel, and developers. All network devices, servers, services, and most application processes are monitored from the dedicated monitoring host.

The Site Reliability (SR) team monitors the Production network 24x7 and is on call for issue resolution. Any potential issues identified by the monitoring tools provide visual and/or email alerts to SR and other appropriate technical operations personnel. Alerts trigger analysis and response procedures. Further notification using established procedures may be executed based on the severity of the issue. In the event of an operational issue, Salesforce's goal is to rapidly restore service.

Management and operations of the Production network is a coordinated effort between the technical operations teams. Several system and application performance monitoring tools are used in the environment. Network devices, servers, services, and application processes are monitored with appropriate tools. Data is aggregated into an event monitoring tool which performs alerting and event correlation.

Other infrastructure and application performance monitoring tools:

- monitor capacity, load, and system events on production systems
- monitor application performance
- monitor end user experience with Force.com applications and services
- query and analysis of raw application logs to identify user specified events

Customers can see uptime and performance of their instance at http://trust.salesforce.com.

System and User Documentation Requirements

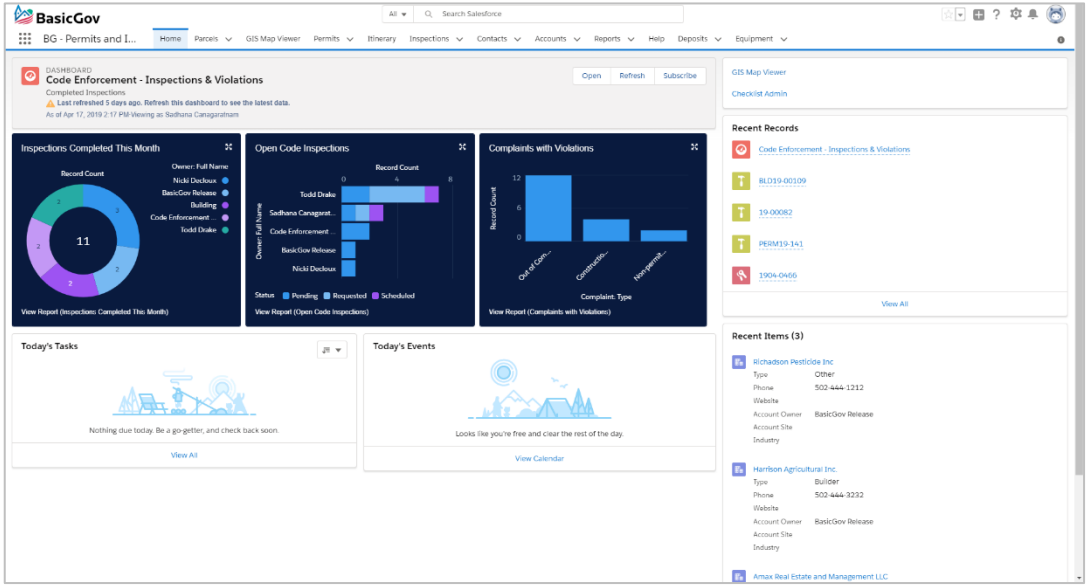
DHHS requires the Contractor to develop, electronically store and distribute system documentation to include, at a minimum:

1. Reference Materials
2. System Documentation
3. A complete Data Dictionary

The Contractor must provide a complete Data Dictionary. The Data Dictionary is to include definitions of all data elements and tables where they reside.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-1	Describe how the system provides on-line help for all features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. Provide a sample copy of five (5) screen shots with on-line help.	X	X		
Response: The BasicGov platform provides a robust help and training portal which brings together a rich set of resources that would give the State a centralized way to help solve problems quickly and easily. We also provide context-sensitive help icons throughout our application screens to make it easier for users to get unique help without searching. The Help site is fully customizable - The State can personalize Help to meet their specific needs, customizing the gadget layout to show what is important to you. Customized help can act as a question and answer flow to assist and guide system users. Salesforce help is publicly available at https://trailblazer.salesforce.com/. Through the portal, users may search through the myriad of documentation that is available, follow online training courses and exercises, or join a community of fellow users and ask questions. BasicGov follows the Salesforce training and documentation model and provides a complete online portal for users and partners for both training and documentation.					
DOC-2	Describe how the system provides on-line user reference materials with a printable version available. The documentation must include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen. Provide a sample copy of five (5) pages of the user reference materials.	X	X		
Response: Both the BasicGov and Salesforce training documents provide reference materials with screen views and windows along with narratives of the features. Due to the configurable nature of the platform, each view is distinct and the number of windows that can be created is near unlimited. Reference materials can be found at the following link: https://help.salesforce.com/home					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-3	Describe how the system will have on-line reporting reference materials with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles. Provide a sample copy of five (5) pages of the reporting reference materials.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The BasicGov system is designed to make it easy for clients to develop their own queries, analytics, dashboards, and ad hoc reports using Report Builder. BasicGov applications provide unparalleled data access through the built in-reporting functionality available in the platform. The platform provides the ability to generate ad-hoc reports on the fly using an easy-to-use report configuration wizard. The Report Builder turns agency data into navigable and usable information that can be presented in easy to use drill down, interactive, and graphical displays. Ad hoc queries can be created as views or as reports. Views can be saved for re-use from a dropdown list of available views without the use of the Report Builder.  The Salesforce Report Builder and Dashboards provides drag and drop functionality to allow users to run saved reports or define new reports and filters to create ad-hoc queries. Users in authorized roles can maintain reports and save as templates to folders. Other system users are granted access to report folders through security profiles and can use the saved templates (which include columns and filters) to run reports. Authorized users can edit existing reports and save the updated templates to folders for other system users to access. In addition to editing a template, authorized users may also clone a report template to make another version of the template and then update the design to create a new template. Reports can be scheduled, and the output emailed to a valid Salesforce user as a .csv or .xls file. More details can be found at: https://help.salesforce.com/articleView?id=analytics_overview.htm&type=5				
DOC-4	Describe how the system provides an entity-relationship model, class diagram, and a table of contents with data dictionary for report creation by the State that is regularly updated and includes table, field, and relationships.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: The BasicGov platform provides an entity-relationship model. Data objects built in the platform support multiple lookup relationships and master-detail relationships. Lookup relationships can be one-to-one or one-to-many as could be exemplified by one business account having multiple licenses associated with it. The platform has a Schema Builder tool that provides a dynamic environment to add new custom objects, custom fields, and relationships to your schema. Schema builder is a tool that lets you visualize and edit your data model. This eliminates the need to click from page to page to find the details of a master-detail relationship or to add a new custom field to an object in your schema. For example, if you're using Schema Builder to view the details of your schema, you can add a new custom object without leaving Schema Builder. The drag-and-drop interface lets you easily add a custom object or new field and saves the layout of your schema any time you move an object. Schema Builder provides details such as the field values, required fields, and how objects are related by displaying lookup and master-detail relationships. You can view the details for both standard and custom objects in Schema Builder.					
DOC-5	Describe how the system provides a data dictionary which includes user-defined fields and tables which can be viewed online and kept updated for each modification.	X	X		
Response: The Schema Builder provides the online data dictionary for the platform and is updated with each modification automatically.					