Diversified Service Network, Inc. (DSN)
2760 Forgue Drive, Suite 100
Naperville, IL 60564
(630) 983-9819
www.dsnworldwide.com

1816

STATE OF INDIANA

Request for Proposal 24-78771

Indiana Department of Administration

On Behalf Of
Family and Social Services Administration

Solicitation For:

Cost Allocation Services

Due Date and Time: March 29th, 2024 by 3:00 PM ET

Appendix: 2.3.12 a and b Business Proposal—Disaster Recovery and Security Plan

Proposal Prepared by:

Diversified Services Network, Inc.

2.3.12 A.

DSN maintains a comprehensive business continuity and disaster recovery plan for itself. and for all client project work as well. DSN has long understood the necessity of quickly re-establishing business operations should any business outage occur – either small or disastrous. DSN has always strived to find quick and practical solutions to ensure business continuity and timely disaster recovery procedures to ensure that not only do our home office operations quickly recover, but that our client projects are minimally affected as well.

DSN's Business Continuity and Disaster Recovery Plans for its Core Business Operations

DSN has long implemented strategies and solutions to minimize the impact of any outage that might affect our ability to conduct business in a timely manner. DSN has implemented multiple levels of protection against such potential events. Some of the implemented business continuity strategies include:

- All *DSN RMTS®* services and databases are hosted on Microsoft Azure and backed up regularly in different regions.
- DSN uses Microsoft Office 365 and Microsoft Azure for its email, SharePoint, webhosting, and database servers. This provides additional security as well as the ability to work anywhere in the case of a disaster. Microsoft Azure has a 99.9% uptime SLA.

The above is just a partial list of the strategies and solutions that DSN has implemented as part of our comprehensive business continuity and disaster recovery plans. Our full business continuity and disaster recovery plans include addressing the most minor of business outages to major catastrophes. DSN's management and client project managers are all trained on addressing any business outage directly, or else quickly escalating any issue up the management chain to ensure that every issue is handled immediately.

DSN would be glad to provide additional details of our comprehensive disaster recovery plans, should you desire.

In conjunction with DSN's core business continuity and disaster recovery plan, we have similar plans associated with providing business continuity and disaster recovery for all client projects. Of course, DSN coordinates all of its disaster recovery efforts for client projects with the client's representatives to ensure that these vital projects become fully operational as quickly as possible. DSN's comprehensive disaster recovery plan begins with ensuring that no client sensitive data is stored on individual hard drives, but instead is stored on a secure and web-accessible cloud-based file storage (i.e., Microsoft OneDrive) for easy access in a disaster. DSN has spare laptops available to ship to our consultants should a consultant's computer fail or be destroyed.

In the event of any disaster that impacts a client project, the management leadership team overseeing the project will get involved in putting the wheels in motion to quickly resolve the issue and ensure that the project begins operating as soon as possible. For the FSSA Cost Allocation Services project, DSN's project leadership team will address any project continuity issues and escalate matters as follows:

Mission Critical Hierarchy of Personnel Functions

Tier 1

- **Karen Kinder, FSSA's Project Manager**
- DSN's local project manager will be the first tier of mangement to assess any project continuity issues or disasters. If there is a need to escalate any issue further, or if Ms. Kinder is not available, communications will go onto 2nd tier of DSN's leadership

Tier 2

- **Nick Petrone, FSSA's Engagement Manager**
- As the Engagment Manager, Mr. Petrone will be the second tier of management to assess any project continuity issues or disasters. If Mr. Petrone is unable to resolve the matter, or if Mr. Petrone is not available, communications will go onto 3rd tier of DSN's leadership

Tier 3

- **Hasan Alpan, DSN's Director of Operations**
- As DSN's Directior of Operations, Mr. Alpan will be the third tier of management to assess any project continuity issues or disasters. If Mr. Alpan is unable to resolve the matter, or if Mr. Alpan is not available, communications will go onto 4th tier of DSN's leadership.

Tier 4

- **Nabil Refai, DSN's Vice President**
- As DSN's Vice President, Mr. Refai will be the fourth tier of management to assess any project continuity issues or disasters. If Mr. Refai is unable to resolve the matter, or if Mr. Refai is not available, communications will go onto 5th tier of DSN's leadership.

Tier 5

- **Taghreed Refai, DSN's President**
- As DSN's President, Ms. Refai will be the fifth and final tier to address any project continuity issues or disasters.

****All key DSN staff have been cross trained in several different areas within our organization. Several staff members can step in to perform day to day operational duties to ensure little to no interruption of ongoing projects or day to day operations occur. *****

Minimization of Downtime and Data Loss Prevention

DSN's business continuity and disaster recovery plans for client projects are designed to minimize and downtime that may occur with an outage, and to also prevent any client data loss. DSN utilizes Microsoft's cloud-based technologies, and its built-in redundancies and guaranteed up-time, to ensure that client project data is secured and easily and quickly accessible from multiple locations in case of disaster recovery or other project disruption.

Some key aspects of how DSN's disaster recovery plans are focused to minimize the impact on client project are as follows:

Downtime Minimizaion	DSN has a policy where all staff has been cross-trained so a fellow staff member can quickly step in the event of a disaster to help minizine the downtown of any project. This ensures a quick ramp up of personnel on any client project to guarantee little to no disruption of the project's timelines. Cross-training is embedded within the DSN's culture to ensure all operations will continue in the event of a disaster. All DSN operations are cloud-based utilizing Microsoft Azure for web and databases, Office 365 for SharePoint and email, allowing team members to set up anywhere minimizing any downtime of a project. Microsoft Azure has a 99.9% uptime SLA. DSN follows stringent security protocols when work is done off-site and remotely.
Data Loss Prevention	All DSN operations and data are protected and automatically backed up via Microsoft Azure and Office 365.

Communications Plan

DSN has a formal internal communications plan developed in the event of disaster to convey key information to all staff and clients. All communications must be approved by higher management to ensure consistency and precision on the message being conveyed.

All DSN staff and clients have contact information of onsite staff and key management staff to contact in the event of a disaster. Contact information will be provided in electronic and hard copy basis.

. DSN's communication plan addresses the following topics to make sure communications run smoothly in an event of a disaster:

1. Contact information of DSN's Crisis Communication Team—Led by our President, Vice President, and Director of Operations
2. Pre-identified Crisis Spokesperson—each project will have a designated spokesperson to address the project team and client in the event of a disaster.
3. Pre-identified Crisis and Proactive Planning—DSN's management has developed a series of disaster scenarios where key management and key personnel brainstorm potential disaster scenarios that could impact projects or DSN's operations.
4. Develop a crisis communications response plan with the key personnel and communication goals of how to handle the disaster.

5. Identify key systems to notify key internal and external personnel of critical communications.
6. Develop templates for key messages to be shared to stakeholders.
7. Review Process to see areas to improve communication.

Alternative Worksite Locations

To ensure work is not disrupted in the event of a disaster, all staff are given DSN secured laptops to work with remotely in their homes. DSN also has several office locations, with a local office in Indianapolis, IN as well, which allows all DSN staff to quickly react in the event of any disaster. As an alternative, should a larger disaster occur, DSN is equipped to move the project to an alternate DSN office facility to ensure that the client project continues with as little disruption as possible.

Microsoft Azure and Office 365 SharePoint make it possible to access databases and Servers from any location with active internet in the event of a disaster.

Securing Data and State Information

2.3.12 B.

DSN RMTS® Web and Data Security Procedures (Hosted on DSN's Microsoft Azure Server)

Purpose:

The purpose of this document is to explain the web and data security procedures for the DSN-Hosted *DSN RMTS®* Application.

Scope:

DSN's procedure will explain the standard methods used and routine/semi-routine processes that are done regarding web and data security with the *DSN RMTS®* system.

Roles:

RMS Administrator

- Answers the phone, e-mails, first level of support for the RMS system.
    - Ensures that samples are being answered, answers samples via employee request, validates samples.
- Verifies that samples are consistent with job classification.
- Produces regular reports.
- RMS Administrator could be DSN or State staff.

Sampled State Employee

- A State Employee that is to be included in the sample.
- The employee will receive web links to respond to their sample during their regular work schedule.

State RMS Coordinator

- Primary State RMS contact.
- Identifies and/or implements changes to employees, regions, locations, work schedules, and job classifications.
- The State RMS Coordinator can also access real-time and quarter-end finalized reports.

DSN's Software Developer

- Maintains and upgrades *DSN RMTS®* Software, Employee Response Website.
- Sets up new implementations and handles bug and software issues.

System Access Infrastructure

The *DSN RMTS®,* SQL Server database is accessed indirectly by the *DSN RMTS®* Desktop Client, the *DSN RMTS®* Web Response Form (Sampled Employees).

DSN RMTS® Desktop Client:

The *DSN RMTS*® Desktop Client is used to administer and manage the *DSN RMTS*® system. The software is used by DSN staff or licensed client. The software must be installed and must have a valid IP Address (DSN staff manage valid IP Addresses for software access).

The software connects to the *DSN RMTS*® database on Microsoft Azure via an encrypted connection. A valid username and password are required. See below for password requirements. An active and stable internet connection is needed to properly use the *DSN RMTS*® Desktop Client.

DSN RMTS® Web Response Form:

- The *DSN RMTS*® Web Response Form is used to respond to Random Moment notifications.
- The Web Response Form is used by Sampled State Employees.
- The user is sent an e-mail notifying them of the sample with a web link to respond. No username or password is needed.
- The weblink contains a Period ID, unique Sample Moment ID, and a randomly generated 32-character hexadecimal security key specific to that Sample Moment. If any of these items are missing or incorrect, the web page will not function correctly.
    - Validations have a different 32-character hexadecimal key.
- Web Response Form links cannot be used for anything other than answering that specific sample.
- Once the sample has been responded to, no additional changes can be made unless the RMS Administrator resets the sample.
- If the sample link is used again after answering, only the Employee’s name, sample moment, and Program/Activity selections are visible. Comments and Case Information are not available.
- An active internet connection and e-mail address are required to answer samples.
- The web response form works with most smart phones and tablets with internet and e-mail access.
- The *DSN RMTS*® Web Response Form uses 256bit encryption with 2048bit signing.

DSN RMTS® E-mail Generator:

- The *DSN RMTS*® E-mail Generator runs 24x7 and sends e-mails out at the time of the Sample Moment or Validation.
- Reminders can also be set up for unanswered samples.
- E-mails use basic text and are transmitted using TLS – Transport Layer Security to send the e-mails.
- Automated e-mails do not have sensitive data within them.

DSN RMTS® Web Training Test (Optional)

- The *DSN RMTS*® Web Training Test tool requires users to pass a simple multiple-choice test about which Program and Activity to choose based on what scenario.
- If the user hasn't taken the test, that user will be unable to answer Sample Moments. This is optional.
- New users can be required to take this test. After the user goes through the training process, they can take the test.
- An e-mail will be sent to the user with a unique System ID and a randomly generated 6-digit code specific to them and other system values so they can access and take the test.
- The user must be able to pass the test to answer samples.

DSN RMTS® System User Access Policy

DSN RMTS® Permissions – For use with the *DSN RMTS*® Administration Software

- Active – Minimum access to login and run reports.
- Universe Management – Ability to view and modify (when open) Regions, Locations, Job Classes, Work Schedules, and Employees
- Sample Moments – View and Modify (when open) sample responses.
- E-mail Generator – View and monitor e-mail schedule and status for Active E-mail Samples. Modify E-mail templates, Reminder E-mail templates and settings. Mark e-mails as "sent" or resend e-mails.
- Matrix Management – View and Modify (when open) the Programs, Activities, Allocation Bases, Funding Sources, and Fund Matrix for a period.
- Sample Management – Create and Delete Sample for a period. Sample must be created at the beginning of a period and once created, those sample moments are fixed for the period.
- Administration
  - Period Management – Create and setup Periods – including rules and website settings. Create and modify settings for Web Test and if passing is required to answer samples.
  - Delete Period – Delete Periods – should only be given for a specific and limited purpose. Usually handled by IT Administrator.
  - System Users – Add/Modify/Remove User Access to the system. Reset passwords and unlock locked accounts due to too many incorrect password attempts.
    - DSN controls IP Address Access through Microsoft Azure.
  - E-mail Templates – Add/Modify Manual E-mail Templates

There are a variety of policy options that can be customized to meet each client's needs.

General Access Requirements

- A User must have a password.
- The password must not be the same as the username.
- The User's password will not be visible to RMTS or Database Administrators
- No spaces at the beginning or end of the password.
- All incorrect passwords will be logged.
- System Users can be given discrete permissions (reports, employees…)
- System Users are specific to a client's database and cannot access another client's database or data.
- System Access is removed within 2-4 business hours after State notifies RMTS Administrators to suspend account (effective immediately)

Optional User Access Requirements

- Password must have # minimum characters.
- Password expires in # days.
- Password Requires at least 1 letter (A-Z)
- Password Requires at least 1 number (0-9)
- Password Requires at least 1 upper and 1 lower letter.
- Web Users timeout in # minutes.
- # minute timeout after # wrong passwords in a row.
- Require RMS Administrator user password reset after # wrong passwords in a row.
- Password cannot be the same as the last # passwords.
- Restrict Users unused for 60 days (manual search in User Manager)
- Reevaluate User Access every 60 days (manual)

Sensitive Data, Security, and Backup Policy

Data Over the Web

- The *DSN RMTS®* websites are encrypted and should not contain sensitive data. If notes are submitted on an RMS Response, those notes are not visible if the link is used again.
- Only the user's selection is visible. When sensitive data is transmitted, it should be used through a secured website, VPN, or other encrypted method.
- Sensitive data (like SSN or medical information) shall not be sent over the internet via an unencrypted method.
- Web Response Form links cannot be used for anything other than answering that specific sample and that can only be done once.
- The *DSN RMTS®* database and Web Response Form are hosted on Microsoft Azure with a 99.9% uptime SLA.
- The *DSN RMTS®* E-mail Generator is hosted on Microsoft Office 365 Exchange with a 99.9% uptime SLA. There will be delays if client e-mail/internet access is down at the time.
- Client e-mail providers may have to add rmts@dsnworldwide.com to the safe sender list.

- Only pre-approved IP Addresses can directly access DSN's Cloud Databases as well a valid credentials.
- DSN's RMTS Azure Environment is SOC 2, SOC TSP, ISO 27001:2013, and PCI DSS 3.2.1 compliant and verified by Microsoft Defender for Cloud.

Security Controls and Capabilities

- Microsoft Azure delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure.
- 24 hour monitored physical security. Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- Monitoring and logging. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.
- Patching. Integrated deployment systems manage the distribution and installation of security patches.
- Antivirus/Antimalware protection. Microsoft Antimalware is built-in to Cloud to help identify and remove viruses, spyware and other malicious software and provide real time protection.
- Intrusion detection and DDoS. Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
- Zero standing privileges. Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged.
- Isolation. Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users.
- Encrypted communications. Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.
- Transparent data encryption is used on all DSN Cloud Databases. Transparent data encryption encrypts our databases, backups, and logs at rest.
- Microsoft Defender for Cloud is used to identify and resolve any security vulnerabilities. Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and cloud workload protection solution that finds weak spots across the cloud-based configuration, helps strengthen the overall security posture of the environment, and can protect workloads from evolving threats. Vulnerability assessments and security audits are performed regularly.

Client Data

- The data is the property of the client and will not be shared with any other party nor used for any other purpose than is agreed upon.
    - Client Production data should not be copied or used elsewhere.
- Sensitive information shall not be kept on an unencrypted PC or ever on an unencrypted flash or hard drive.
- Sensitive information not needed to be retained shall be scrubbed (deleted and overwritten)
- Security Breaches shall be reported to the client within 1 business day or sooner upon identification.
    - Identified Security Breaches (Confirmed or Potential) will be logged in Microsoft Sentinel, if not automatically generated.
- Upon discontinuing *DSN RMTS*® Hosted, the Employee Response data (and other details) will be provided to the client in table-based MS Excel or SQL Server database export.