Small Business Administration
Office of Performance Management For

Evaluation of the T.H.R.I.V.E. Program

Note: This is an Official SSP, and it represents the security of controls as of:

Created Date: 6/21/22

Contents

1. Information System Name/Title:

System Name: Evaluation of the T.H.R.I.V.E. Program

Acronym: THRIVE

UID: 73351022F0048

System Type: Information System

XLC Phase: Production

2. Information System Categorization:

Security Category: Moderate

3. Stakeholders:

Business Owner: JoAnn D. Braxton

Chief Information Officer (CIO): Stephen Kucharski (Acting)

ISSO Contractor Support: Lucas, Cordain

Security Control Assessor (SCA): N/A

System Developer Maintainer: N/A

Chief Information Security Officer (CISO): Kelvin Moore

Primary Information System Security Officer: N/A

Deputy Chief Information Security Officer (DCISO): N/A

Cyber Risk Advisor (CRA): N/A

4. Information System Type:

Information System Type: Minor Application [Stand Alone]

E-Authentication Level: N/A

5. General System Description:

Recovery Time Objective (RTO): 72 Hours

Recovery Point Objective (RPO): 24 Hours

Work Recovery Time (WRT): 24 Hours

Maximum Tolerable Downtime (MTD): 96 Hours

Information Classification: SBA Controlled Unclassified Information (CUI)

Production Operated by: Contractor

Marketplace Systems: No

Primary Operating Location: AWS FedRAMP

FISMA System: Yes

Financial System: Yes

Does this include cloud-based services?: Yes

Cloud Service Provider (CSP): AWS FedRAMP

Authentication Required: Yes

System Description:

Task Order 73351022F0048 seeks Optimal to conduct an evaluation of the T.H.R.I.V.E program. The tasks needed to complete this evaluation include:

- Project Management
- Evaluation Design
- Data Collection and Analysis

- Reporting

The Evaluation of the T.H.R.I.V.E Initiative will be using Optimal's FISMA-Low/FedRAMP server environment to store, manage and manipulate the sensitive data required for the analysis. Section 11 of the SSP includes the list of staff with access to the FedRAMP server environment. Additionally, activities under the evaluation will use Optimal's SharePoint site to store and manage files (non-sensitive data) and only approved Optimal staff will have access to the files on the SharePoint. List of approved staff are in included in the Management Work Plan.

System of Records Notice (SORN): N/A

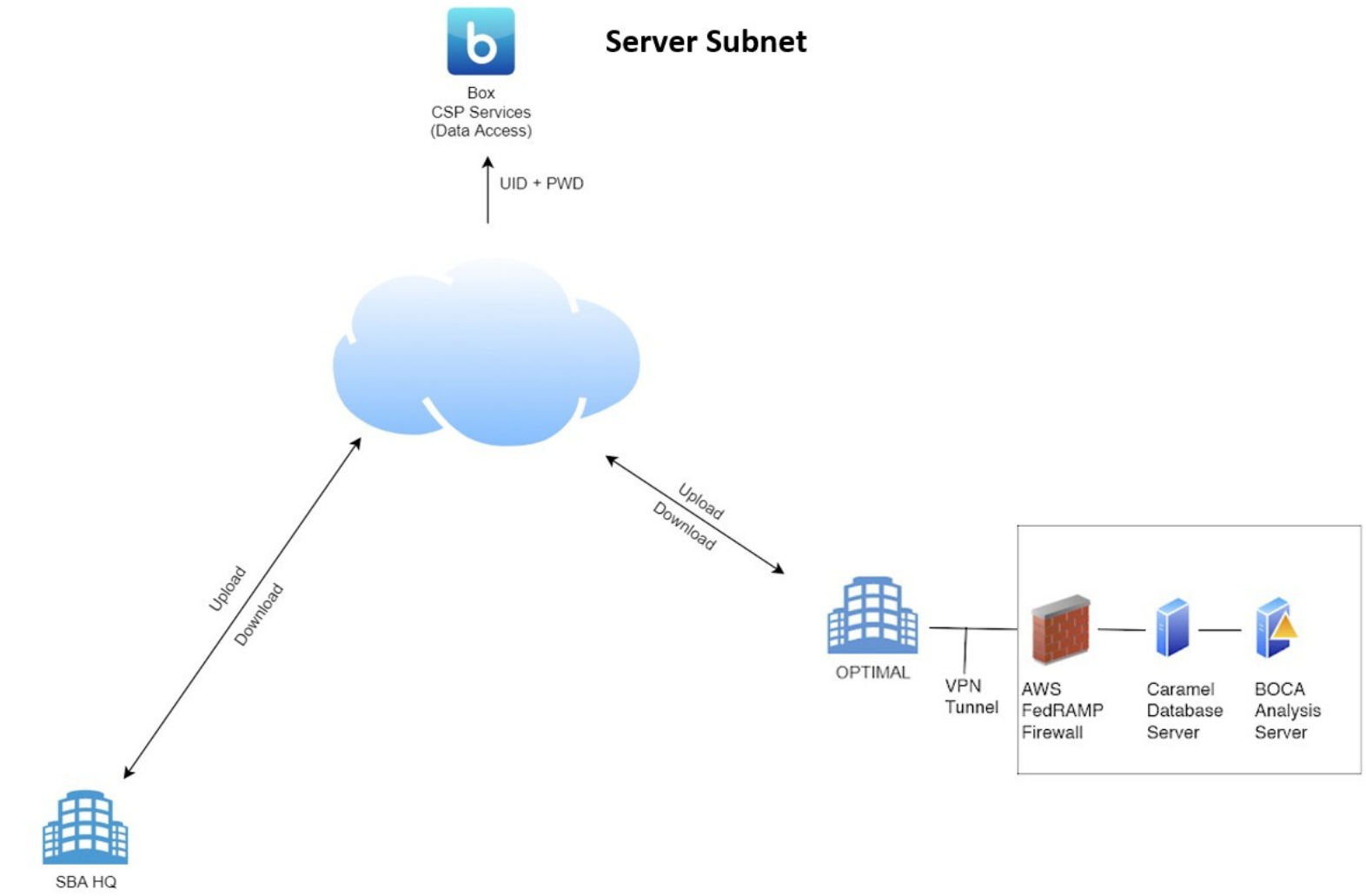
6. Information Types:

Information Type Name	Confidentiality Rating	Integrity Rating	Availability Rating	Description
C.2.1.2 Program Evaluation	Low	Low	Low	Program Evaluation involves the analys internal and external program effective and the determination of corrective act as appropriate.
C.2.1.3 Program Monitoring Information Type	Moderate	Moderate	Moderate	Program Monitoring involves the data-gathering activities required to determi the effectiveness of internal and extern programs and the extent to which they comply with related laws, regulations, a policies. The impact levels should be commensurate with the impact levels o programs that are being monitored. Fo example, if a program contains very sensitive financial data with moderate impact levels for confidentiality and integrity, the program monitoring impa levels for confidentiality and integrity should also be moderate.
C.2.3.6 Workforce Planning Information Type	Low	Low	Low	Workforce Planning involves the proces for identifying the workforce competen required to meet the agency's strategi goals and for developing the strategies meet these requirements.

7. Boundary Details:

Authorization Boundary Description:

The T.H.R.I.V.E contract authorization boundary consists of the Optimal corporate IT workstations/laptops, the SBA IT systems and a virtual server hosted on a FedRAMP certified Cloud Service Provider (CSP), AWS FedRAMP. All transport is encrypted using TLS over port 443 through a secure VPN, all data is hosted on a virtual server which is also encrypted, in a FedRAMP Moderate government rated environment.



Note: CSP - Cloud Service Provider
DC - Domain Controller
HQ - Head Quarters
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
PWD - Password
RDP - Remote Desktop Protocol
SQL- Structured Query Language
UID - Unique Identifier
VPN - Virtual Private Network

Production LAN:

i. Server Subnet 1 – Caramel
    1. Operating System: Windows Server 2019 64 bit
    2. Software installed
        i. Stata MP 64-bit, version 14.2
        ii. Microsoft Excel, version 15.0.5059.1000
        iii. R, version 3.4.3.2606
        iv. Rstudio, version 1.1.456
        v. Sourcetree, version 2.6.10
        vi. 7zip, version 19.00
        vii. Fileshredder, version 2.5

ii. Server Subnet 2 – Boca
    1. Operating System: Windows Server 2019 64 bit
    2. Software installed
        i. NVIVO 10
        ii. 7zip, version 19.00
        iii. Fileshredder, version 2.5

8. System Interconnections/Information Sharing:

Interconnection Name	Type	Date of Agreement	Information being exchanged description	Connecting Third Party	Connecting Information System
N/A	N/A	N/A	N/A	N/A	N/A

9. Data Transmission workflow

To ensure the secure identification and storage of data in the system, Optimal will use the following workflows.

Data Storage

To store personally identifiable information (PII) and sensitive data received via an approved means of transmission, Optimal will use the FedRAMP-approved virtual server. The physical server is located at AWS FedRAMP's physical location. The virtual server is only accessible on Optimal's network and each Optimal team member has unique login credentials:

1. The list of authorized users is provided in each task order's MWP.

Data Transmission

To transfer PII and sensitive data files between the SBA and Optimal, Optimal and the SBA will use the following controls and processes:

1. To transfer any sensitive files or files that contain PII, the SBA will upload the files to its File Transfer Protocol System (FTPS) and provide Optimal with the link to the files through email. Optimal will then access the FTPS link from the SBA on the virtual server. The files will be directly downloaded to the virtual server's hard drive for storage and analysis.

    a) Files must be encrypted using 7-Zip or another AES-256 level encryption software.

    b) The encryption key must be provided to an authorized Optimal team member via a phone call. The encryption key will not be sent together with the encrypted file.

2. In the event that the SBA no longer utilizes its FTP; to transfer sensitive files or files that contain PII, Optimal will ask the SBA to send the files through physical mail on a CD, DVD-ROM, thumb drive, or other physical multimedia.

3. Files that are non-sensitive (as verified by the SBA) or determined to be free of PII can be uploaded to Optimal's Office 365 SharePoint or another secure server.

4. No PII/CBI/sensitive information that is stored on the FEDRamp server will be downloaded off the server for any analysis, storage, or other purposes

Optimal will supply the final programming files and datafiles to the SBA upon completion of each task order under the RIC contract. The final datafiles will be provided in proprietary and nonproprietary format. A csv file of the data, with associated codebook, will be provided along with the Stata version of the data, which can be imported into SAS using the proc import command. Importing the Stata data file into SAS directly will inhibit the loss of information, such as variable value labels. Any datafiles

transferred to the SBA that contains sensitive information will be encrypted using AES-256. The encrypted file will be uploaded to the SBA's Box account using FTPS. Optimal will send the password to the encrypted file to the SBA via phone call. If the files are too large Optimal will provide physical drives (CD, DVD, thumb drive, etc..) with the files to the SBA through mail.

Data Backup

Server configurations allows for daily shadow copies of drives. This allows for timely restoration of data in the event of a drive-level, folder-level or drive-level data compromise. In addition, there is a daily snapshot server policy in place to capture the entire server. This will allow for a complete server restoration in the event of the server being compromised.

Data Breach

In the event of a suspected unauthorized disclosure or breach, the Optimal team will follow guidelines specified in the SBA SOP 90 501 Breach Notification Response plan as well as procedure provided in the Optimal Event Incident Response Plan.

Data Disposal

To dispose of data, Optimal will use the FileShredder software, located on the virtual server, three years after project completion, unless requested earlier by the SBA. FileShredder permanently deletes files, and temporary files associated with the permanent files, from all locations of the hard drive. In addition, the virtual server will be deleted, and the physical hard drive wiped using the DoD wipe procedure.

Data Use

Optimal will opt out of the use of SBA's data for any other purposes other than what is described in the evaluation methodology. Optimal will remove any PII associated with the interview recordings before uploading the recording to any other application for transcription purposes. Optimal will immediately delete the uploaded interview recordings from Otter.ai after transcription is completed.

10. Related Laws/Regulations/Policies:

A. Privacy Act of 1974 (5 U.S.C. § 552a)

B. Freedom of Information Act (5 U.S.C. § 522b)

C. Federal Managers Financial Integrity Act of 1982 (31 U.S.C. § 1352)

D. Paperwork Reduction Act of 1986 (44 U.S.C. 35)

E. Electronic Communications Privacy Act of 1986 (P.L. 99-508, as amended; codified in 18 U.S.C. chapters 119, 121 and 206)

F. Computer Fraud and Abuse Act of 1986 (P.L. 99-474, as amended; codified at 18 U.S.C. § 1030)

G. Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) (Division E of P.L. 104-106, as amended; codified in part in 44 U.S.C. chapters 111, 113, 115 and 117)

H. Title III of the E-Government Act of 2002 (P.L. 107-347) and Federal Information Security Management Act of 2002 (FISMA) (P.L. 107-296; codified in part in 44 U.S.C. chapters 35 and 36)

I. Computer Security Act of 1987 (P.L. 100-235, as amended)

Office of Management and Budget (OMB) Circulars and Bulletins

A. Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control, Dec. 21, 2004, OMB Circular A-127, Financial Management Systems, revised July 23, 1993;

B. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Transmittal #4, Security of Federal Automated Information Resources, Nov. 28, 2000;

C. Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities (COOP Plans), Nov. 18, 1988, as amended by EO 13074, Feb. 9, 1998;

D. EO 13011, Federal Information Technology, July 16, 1996;

E. OMB Circular No. A-130, Appendix III establishes a minimum set of controls to be included in the Federal automated information security programs and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123;

F. OMB Bulletin 90-08, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems that Contain Sensitive Information, July 9, 1990;

G. Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection;

H. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors;

I. Presidential Decision Directive (PDD) 67, Continuity of Government (COG) and Continuity of Operations (COOP) Plans Practices for Securing Critical Information and Information Systems and Networks, 1988;

J. M-03-22 – OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;

K. M-05-16 – Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally-owned Buildings;

L. M-06-16 – Protection of Sensitive Agency Information;

M. M-06-20 – FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management;

N. M-06-15 – Safeguarding Personally Identifiable Information;

O. M-06-19 – Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments;

P. M-07-11 – Implementation of commonly Accepted Security Configurations for Windows Operating Systems, March 22, 2007;

Federal Information Processing Standards Publications (FIPS PUBs) & National Institute of Standards and Technology (NIST) Special Publications

A. FIPS-201, Personal Identity Verification (PIV) of Federal Employees and Contractors;

B. FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems;

C. FIPS PUB 200, Minimum Security Requirements for Federal Information Systems;

D. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems;

E. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal information Systems;

F. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, and referenced supplemental guidance documents;

G. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories;

(See following link: http://www.nist.gov/index.html)

11. Training Status of Staff with access to Optimal's FedRAMP environment

Server Access

The server can only be accessed through an industry-standard, AWS FedRAMP VPN client running on a firewall, using AES-256 encryption between the server and the duly authorized end-user machine. The user will ONLY access the data on a local machine owned by Optimal Solutions Group, as the AWS FedRAMP VPN client will be configured with Optimal's unique Profile Configuration File (PCF) and no other. This will prevent users from accessing the server on any machine not subject to the security protocols of Optimal Solutions Group. In order to login to the server, the user will have to already have been set up with a VPN login and password, as well as accessing from a registered Optimal machine with the necessary .PCF file configured in the step above. The user will open the VPN tunnel, allowing a secure Remote Desktop Connection to the server. All data will remain on the server, with NO data exchanged between the server and the local PC from which the user will access the server. The user will ONLY access the data ON the server remotely. The server will be protected from the outside internet via industry standard hardware firewall, affording complete network isolation from both the Internet, and Optimal's internal network LAN. These factors together will ensure the server remains completely standalone and isolated, only authorized users can login to the server, and the integrity of the data is never compromised.

Training Status

All staff will complete applicable trainings before commencing work on this project. Training status will be provided on a monthly basis as part of the monthly progress report.

In the event of change in staff, an email will be sent to the SBA with the following information:

1. Name of on-boarding/off-boarding staff.
2. Date of on-boarding or on-boarding.
3. Role of the on-boarding/off-boarding staff.
4. If off-boarding, replacement plans.

In the event of a change in key project staff, Optimal will submit a formal memorandum requesting the change. Additionally, Optimal will also document the staff change in monthly progress report.

Staff and Training Status

Staff Member	Cybersecurity and Privacy Awareness Training Completed	CITI / HIPAA Training Completed
Andrey Vinokurov	12/2021	4/2022
John Foster-Bey	12/2021	4/2022
Mark Turner	1/2022	^
Cordain Lucas	12/2021	^
Daniel Gluck	12/2021	12/2021
Oswaldo Urdapilleta	4/2022	4/2022
Prathamesh Sharma	12/2021	^
Jatan Rathod	5/2022	^
Sagar Anvekar	2/2022	12/2021
Sadaf Asrar	2/2022	12/2021
Nicholas Bahel	5/2022	5/2022

* OMO security training fulfills the requirements of NIH training

^ Only Research Staff are required to complete this program

12. Information System Security Plan Completion Date:

Completion Date: 6/21/22

13. Information System Security Plan Approval Date:

Approval Date: TBD