Division of Operations and Systems

System Security Plan (SSP) Workbook for

Moderate Plus Impact Level Controls

System Overview

Version 3.1.05

June 1st, 2021

Record of Changes

Date	Author	Description of Change	Version
01/01/2019	R. Wheeler	Initial	3.1
06/01/2021	R. Wheeler	Refreshed	3.1.05

Table of Contents

Executive Summary

A System Security Plan's executive summary should be a short, direct description appropriate for executive-level readership. The summary should provide a high-level understanding of what the system is, what sensitive data it processes and/or stores, and what key protections have been applied. An executive summary must not exceed one (1) single-spaced page. The general rule is, "the shorter, the better." Please do not restate procedure. Summarize the important, relevant facts about the system's essential business processes, the general security strategy, and the overall security posture as previously described.

"[Click here and type text]"

1. System Identification

1.1 System Name, Title and Location

Provide the system identifier, which includes the official name and/or title of the system, including any commonly used acronyms.

Table SSP-1. System Name, Title, and Location

System Identifier	Response Data
Official System Name:	
System Acronym:	
Provide the street address where the system physically resides.	

1.2 Responsible Organization

Provide contact information for the organization(s) responsible for the system. The following contact information should be provided in Table SSP-2 for internal as well as external organizations.

Table SSP-2. Responsible Organization

Entity	Response Data
Internal	
Name of Organization:	
Address:	
City, State, Zip:	
Contract Number:	
Contract Name:	
External	
Name of Organization:	
Address:	
City, State, Zip:	

Entity	Response Data
Contract Number:	
Contract Name:	

1.3 Designated Contacts

Indicate the names of other key contact personnel who can address inquiries regarding system characteristics and operation. Required contacts include, but are not limited to, Business Owner, System Developer/Maintainer, SSP author, (or equivalent), etc. The SSP should include the following contact information in Table SSP-, Table SSP-, and Table SSP- for each of the Designated Contacts.

Table SSP-3. Designated Contacts: Business Owner

Business Owner	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-Mail:	
Phone Number:	
Contractor contact information (if applicable):	

Table SSP-4. Designated Contacts: System Developer/Maintainer

System Developer/Maintainer	Response Data
Name:	
Title:	
Organization:	

System Developer/Maintainer	Response Data
Address:	
City, State, Zip:	
E-Mail:	
Phone Number:	
Contractor contact information (if applicable):	

Table SSP-5. Designated Contacts: System Security Plan Author

SSP Author	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Contractor contact information (if applicable):	

Identify and add a table for any additional personnel who can address system-related inquiries. Provide titles and contact information for each.

1.4 Assignment of Security and Privacy Responsibility

Identify one (1) primary security Point of Contact (POC) and one (1) alternate or emergency, Point of Contact. The assignment of security responsibility shall include the following information in Table SSP- and Table SSP-. Identify the primary privacy POC and one (1) alternate, or emergency, POC in Table SSP- and Table SSP-, respectively.

Table SSP-6. Primary Security POC

Primary Security POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact: (name, phone & email)	

Table SSP-7. Alternate Security POC

Alternate Security POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

Table SSP-8. Primary Privacy POC

Primary Privacy POC	Response Data
Name:	

Primary Privacy POC	Response Data
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact: (name, phone & email)	

Table SSP-9. Alternate Privacy POC

Alternate Security POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

1.5 System Operational Status

Note in Table SSP-10 whether the system is New, Operational or Undergoing Major Modification.

Table SSP-10. System Operational Status

System Operational Status	Response Data

Select one System Operational Status from the following: New, Operational, or Undergoing a Major Modification.	

1.6 Description of the Business Process

Provide a brief description of the business process as it is supported by the system:

- **Describe the business function for each system.** Provide information regarding the overall business processes, including any business process diagrams and/or workflow diagrams.
  - Describe the underlying business processes and resources that support each business function. This may include the required inputs (business functions/processes that feed this function), processing functions (calculations, etc.), organizational/personnel roles and responsibilities, and expected outputs/products (that may "feed" other business functions / processes).
  - Describe how information flows through/is processed by the system, beginning with system input through system output. In addition, describe, for example, how the data/information is handled by the system (is the data read, stored, and purged?).
- **Indicate the organization (internal and external), and the type of data and processing that will be provided by users, if any**.
  - Describe different user roles and associated levels of access to system-related data (read-only, alter, etc.), system-related facilities, and information technology resources.

"[Click here and type text; include diagrams as necessary]"

1.7 Description of Operational / System Environment and Special Considerations

1.7.1 Operational Information

Describe at a high level the anticipated technical environment and user community necessary to support the system and business functions. Include in this description any:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Be sure to indicate the physical location of the business processes and technology that will support the system.

"[Click here and type text]"

1.7.2 System Information

Provide a brief, general description of the technical aspects of the system. Include any environmental or technical factors that raise special security concerns, such as the use of Personal Digital Assistants, integrated wireless technology, etc.

- Describe principal hardware components.
- Describe principal software components.
- Describe principal firmware components. (For security and network appliances)
- Describe principal encryption solutions and public key infrastructures.

"[Click here and type text]"

"[Click here to include the system diagram]"

Attach the network connectivity diagram(s) that shall address the system component connections and security devices, which (1) protect the system and (2) monitor system access and system activity. Include an input/output diagram. For systems that have more than one server of the same type, only include one in the diagram; however, provide an accurate total count of servers in the supporting text description. Be sure to provide an introductory sentence(s) that describes the diagram.

"[Click here and type text]"

Following the diagram, include text that will explain the various system components and their functionality. Be sure to annotate system components in the diagram to correlate specific graphic depictions with the information provided in the summary paragraph.

"[Click here and type text]"

1.7.3 System Environment

Describe key aspects of the system operating environment beginning with the following key data points in Table SSP-11 and conclude with a detailed discussion of the essential security support structure of the system.

Table SSP-11. System Environment

System Environment	Response
Is the system owned or leased?	
Is the system operated by the State or by a support service contractor?	

System Environment	Response
If the system is maintained by support service contractor, describe comprehensively how the system is managed.	
If the system is operated by the state run consolidated data center, provide the name, location and point of contact for the consolidated data center.	
Provide the hours of operation if this is a facility where the system is hosted: e.g., 24x7, M–F 7:30 am – 5:00 pm.	
Document the approximate total number of user accounts and unique user types (i.e., researchers, programmers, administrative support, caseworkers, and public-facing employees).	• XX Administrator accounts • XX Programmer accounts • XX Caseworker accounts • Etc.
Identify critical processing periods (e.g., eligibility processing).	
If system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies).	
Is FTI being processed or stored in this system?	
List all applications supported by the system including the applications' functions and the information processed.	
Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.	

Use Table SSP-11 to address the following items:

- Provide a description of the system environment: If the system is maintained and/or operated by a contractor, describe (comprehensively) how the system is managed.

- If the system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies, assistors, navigators).
- Describe all applications supported by the system including the applications' functions and information processed.
- Describe how system users access the system (i.e., desktop, thin client). Include any information required to evaluate the security of the access.
- Describe the information / data stores within the system and security controls that limit access to the data.
- Describe the purpose and capabilities of the information system. Describe the functional requirements of the information system. For instance:
  - Are boundary protection mechanisms (i.e., firewalls) required?
  - Are support components such as web servers and e-mail required?
  - What types of access mechanisms (i.e., telecommuting, broadband communications) are required?
  - Are "plug-in" methods (Mobile code; Active-X, JavaScript) required?
  - What operating system standards, if any, are required?

Use Table SSP-12 to provide more details regarding system users including the following items:

- User types
- Organizations (internal and external) comprising the user community
- Users' level of access (e.g., read-only, alter, and the like)
- Uniform Resource Locator (URL) for web-based access
- How the system is accessed

Table SSP-12. System Roles

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	Expected Output / Product	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)	Comments

1.7.4 Architecture and Topology

Describe the architecture of the information system, and include the following information:

- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and describe how these address information security requirements.

"[Click here and type text; include diagrams as necessary]"

1.7.5 System Boundary

Provide a detailed description of the system boundaries and technical components that defend the boundary. The description should contain the following elements:

- Describe the boundary of the information system for security accreditation.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network topology.
- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.
- Following the logical diagram, describe the information flow or processes within the system that provide access to the data/information.

"[Click here and type text; include diagrams as specified below]"

1.7.6 Primary Platforms and Security Software

Describe the primary computing platform(s) used and the principal system components, including hardware, firmware, software, wireless, and communications resources. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). This will include vendors and versions. Include the following:

- Information concerning a system's hardware and platform(s). Detailed hardware inventories shall be submitted as an attachment.
- Any security-relevant software protecting the system and information.
- In general terms, the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented, rather than listing the controls that are available in the software.

"[Click here and type text]"

1.7.7 Interconnectivity Interfaces, Web Protocols, and Distributed and Collaborative Computing Environments

Describe the Web protocols and distributed, collaborative computing environments (i.e., processes and applications), and include a description of the following:

- The connectivity between modules within the scope of this system.
- For any system that allows individual web-based access (Internet, Intranet, Extranet) to conduct transactions, the following information should be provided:
  - The Uniform Resource Locator for the web-based transaction;
  - E-authentication architecture implemented;
  - E-authentication interoperable product used;
  - Other authentication products used;
  - Number of electronic logons per year;
  - Number of registered users (Government to Government);
  - Number of registered users (Government to Business);
  - Registered users (Government to Citizen);
  - Number of registered internal users; and
- Description of customer groups being authenticated, e.g., Business Partners, Medicare Service Providers, and Beneficiaries).

"[Click here and type text]"

1.7.8 Special Security Concerns

Indicate if the system receives, stores, processes, or transmits Federal Tax Information. Appendix A provides a list of IRS requirements for safeguarding FTI. These requirements should be documented in the SSP workbook in addition to the MARS-E security and privacy controls for systems that receive, store, process, or transmit FTI information.

"[Click here and type text]"

1.7.9 Other Special Security Concerns

Include any environmental or technical factors that raise special security concerns, such as:

- The physical location of the information system;
- The system is connected to the Internet;
- The system is located in a harsh environment;
- Software is implemented rapidly;
- Software resides on an open network used by the public; and

- Application(s) is/are processed at a facility outside of the state's control.

"[Click here and type text]"

1.8 System Interconnection / Information Sharing

By definition, system interconnection is the direct connection of two or more IT systems for the purposes of sharing information resources. Business Owners and managers should be acutely aware of, and obtain as much information as possible, regarding all potential vulnerabilities associated with system interconnections or that may result from information sharing. Strong situational awareness is essential when selecting appropriate security and privacy controls.

An Interconnection Security Agreement (ISA) with CMS is required if a system-to-system connection is made to the Federal Data Services Hub (DSH) to exchange data with CMS.

ACA Administering Entity Systems should also maintain ISAs and Memoranda of Understanding (MOU) between all additional IT systems that connect to and share data or resources with the Administering Entity System. Using Table SSP-13, please describe the information sharing agreements in place that govern the data exchange. If not yet finalized, provide the current status.

Provide details about all interconnections where transmissions cross the system boundary (inbound/outbound). This includes systems not governed by this security plan such as:

- Untrusted connections, including connections to the Internet, which require protective devices as a barrier to unauthorized system intrusion. Indicate if the connection is/are government-to-government, government-to-business, government-to-citizen, etc., and describe the controls to allow and restrict public access.
- Trusted connections that do not contain barrier protection devices such as firewalls. Indicate if the connection is/are government-to-government, government-to-business, government-to-citizen, etc., and discuss why the connection is trusted. Reference here and include in the SSP a copy of all MOUs, Memoranda of Agreements (MOA), Service-Level Agreements (SLA), and System Interconnection Agreements for provisioning IT security for this connectivity.

Table SSP-13. System Interconnections

Connecting Entity	System Name	Internal / External	Interconnection Type (How system accessed – TCP/IP, Dial, SNA, etc.)	Authorized Access Agreement in Place (ISA, MOU, BPA, etc.)	Name & Title of Authorizing Management Official(s) and Date of Authorization:	Comments

1.9 System Security Level

Describe in general terms the information handled by the system and associated protective measures. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidelines for categorizing information and/or information systems.

"[Click here and type text]"

1.10 Digital Identity Assurance Level

Information System owners, or any 3rd parties contracted to build on behalf on a NYS agency must complete digital identity requirements assessments during system design to determine the appropriate Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL) for all information technology (IT) systems that will require user authentication and contain or process SE data. The assessments focus on:

- whether the person seeking to access the system is who they claim to be and the potential impact to the confidentiality and integrity of the data and/or system if that person is not who they claim to be;
- whether the person accessing the service today is the same person who accessed the service using the same authenticator previously; and
- how to convey the results of authentication processes and relevant identity information to other applications.

Completion of the assessments provides a system specific numerical IAL, AAL, and FAL.

Assessments must be documented and kept with other system documentation and must be used to guide system design and functions which impact identity, authentication, and/or federation services.

Information system owners should review the following NYS Digital Identity Policy and Standard documents:

NYS-P20-001 Digital Identity Policy

NYS-S20-001 Digital Identity Standard

Indicate the type of E-Authentication Assurance and authentication type used for each user role in the cell for Response Data in Table SSP-15.

Table SSP-15. E-Authentication Assurance Levels

User Role	Assurance Level	Authentication Type
Example Role “Anonymous”	AL-1	None
Example Role “Administrator”	AL-2	Multi-factor Authentication

1.11 Applicable Laws or Regulations

List any laws, regulations, specific standards, guidance, or policies governing the system(s), organizations, and business processes.

"[Click here and type text]"

1.12 Review of Security or Privacy Controls

Provide information regarding any reviews that have been conducted in the past twelve (12) months.

If a security evaluation were conducted within the past twelve (12) months, the following information must be provided:

- The name of the person and organization performing the review;
- The date of the review;
- The purpose of the review;
- A summary of general findings;
- A list of actions taken as a result of the review; and
- A reference to the location of the full report and corrective action plans.

"[Click here and type text]"