U.S. Department of Housing and Urban Development (HUD)

Office of the Chief Information Officer (OCIO)

Interconnection Security Agreement (ISA)

Between the U.S. Department of Housing and Urban Development (HUD)
and
'Organization B'

March 3, 2021

Revisions Record

Version Number	Date	Description of Revision	Section/Pages Affected
1.0	3/3/2021	Draft of the ISA between HUD and Organization B, which is required for production system interconnection	All

TABLE OF CONTENTS

1. INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between the U.S. Department of Housing and Urban Development (HUD) and "*Organization B*" are for the express purpose of exchanging data between the MTW Expansion Application, owned by HUD, and "*System B*," owned by *Organization B*. *Organization B* requires the use of HUD's MTW Expansion Application data and *Organization A* requires the use of *Organization B's "ABC database*," as approved. This Agreement is between U.S Department of Housing and Urban Development (HUD), with its principal place of business at 451 7th Street S.W., Washington, DC 20410 and *Organization B*, with its principal place of business at *<insert location, if applicable>*.

2. SYSTEM SECURITY CONSIDERATIONS

- **General Information/Data Description.** The interconnection between the MTW Expansion Application, owned by HUD, and *System B*, owned by *Organization B*, is a two-way path. The purpose of the interconnection is to exchange data between HUD's MTW application and *Organization B's System B*.
- **Services Offered.** This connection exchanges data between HUD's MTW Expansion application and *Organization B's System B* via a dedicated system to system connection. *Organization B* may also have users accessing the MTW Expansion application via user ID and password, which will be provisioned by HUD through the MTW Expansion application.
- **Security Measures**. Each party must (i) implement and maintain all reasonable security measures appropriate including without limitation, technical, physical, administrative and organizational controls; (ii) implement and maintain industry standard systems and procedures for detecting, preventing and responding to attacks, intrusions, or other systems failures and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (iii) designate an employee or employees to coordinate implementation and maintenance of its security measures; and (iv) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such data, and assess the sufficiency of any safeguards in place to control these risks. HUD systems are assessed and authorized in accordance with guidance from the National Institute of Standards and Technology (NIST), the Federal Information Security Modernization Act of 2014 (FISMA), and other federal standards. Organization B must self-certify that the security posture of the information system(s) covered by this ISA will also follow NIST, FISMA, and other federal guidance, including Federal Risk and Authorization Management (FedRAMP)

requirements as applicable. *Organization B* must provide *Organization A* with results from third-party assessments or attestation annually. Upon review and signature of the MOU and ISA, *Organization B* must send evidence of security reviews and assessments to their counterparts at *Organization A* and / or directly to ContinuousMonitoring@hud.gov. *Organization A* will review the results to ensure the security of the system is acceptable.

- **Data Sensitivity.** The sensitivity of data exchanged between HUD and *Organization B* is personally identifiable information (PII).
- **User Community.** All HUD users with access to the data received from *Organization B* are U.S. citizens with a valid and current HUD background investigation. All *Organization B* users with access to the data received from HUD are U.S. citizens with a valid and current *Organization B* background investigation.
- **Information Exchange Security.** The security of the information being passed on this two-way connection is protected through the use of FIPS 140-2 validated encryption, which protects the data in-transit and at rest. The MTW Expansion application is hosted in the Salesforce Government Cloud (Gov Cloud), which has a FedRAMP Moderate Authority to Operate (ATO) and Department of Defense Impact Level 4 Provisional Authorization (PA). These authorizations enable organizations to transmit, process, and store sensitive information such as personally identifiable information (PII).

  Gov Cloud also provides the following:
  - U.S. Data Centers: Customer Data is processed and stored solely within the continental U.S
  - U.S. Citizens: Operated and supported by screened U.S. citizens as applicable.

  Salesforce's approach to information security governance is structured around the ISO 27001/27002 framework and consistent with the requirements identified in NIST SP 800-53. All users are granted Role Based Access Control (RBAC) and the concept of least privilege is applied to support control and access to data elements within the system. The default user authentication mechanism for the Salesforce Government Cloud requests that a user provide a username and password (credentials) to establish a connection. The Salesforce Government Cloud does not use cookies to store confidential user and session information [AC-2, IA-2].
- **Trusted Behavior Expectations.** HUD's system and users are expected to protect *Organization B's ABC database*, and *Organization B*'s system and users are expected to protect HUD's MTW Expansion application, in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710).

- **Formal Security Policy.** Policy documents that govern the protection of the data are covered by HUD OCIO's IT Security Policy Handbook and *<Organization B's "YYY Policy>*."
- **Incident Reporting.** The party discovering a security incident will report it in accordance with HUD's incident reporting procedures. In the case of *<Organization B>*, any security incident will be reported to the *<information for Organization B>*.
- **Audit Trail Responsibilities.** Both parties are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year.

3. POINTS OF CONTACT

For all issues associated with this ISA, the established points of contact are as follows:

U.S. Department of Housing and Urban Development	***Organization B***
Authorizing Official (AO) Ashley Sheriff	**Authorizing Official (AO)**
System Owner (SO) Matilda Chiu	**System Owner (SO)**
Information System Security Officer (ISSO) Dallas Blair	**Information System Security Officer (ISSO)**
Project Manager (PM) Matilda Chiu	**Project Manager (PM)**

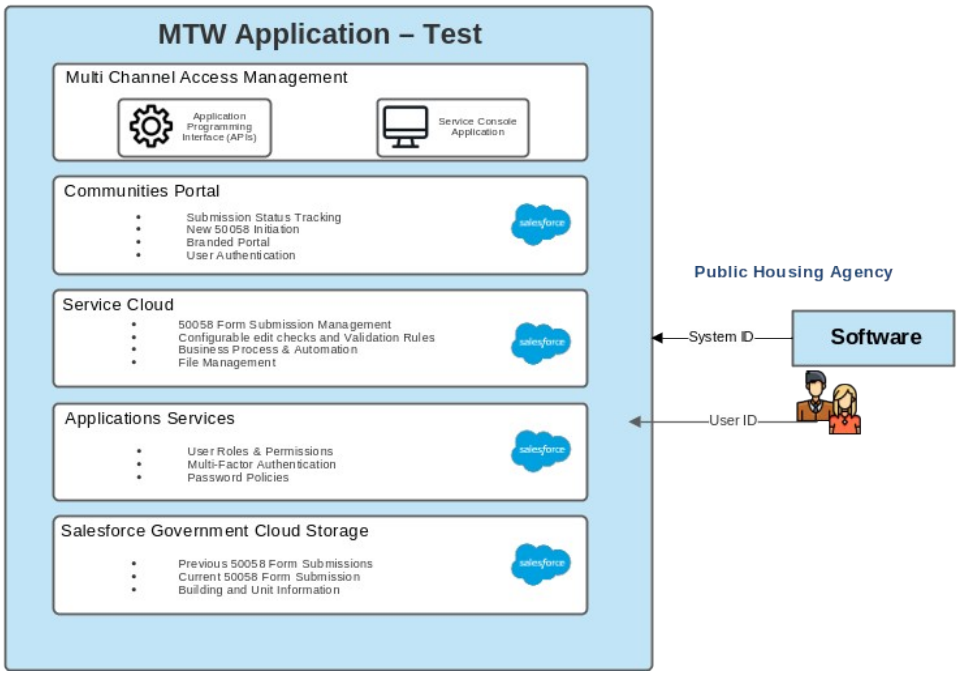
4. TOPOLOGICAL DRAWING

Organization B will submit 50058 data to the MTW Expansion application either through the application, using a user ID and password created by HUD, or via a system to system connection between the *Organization B's system* and HUD's MTW Expansion application.

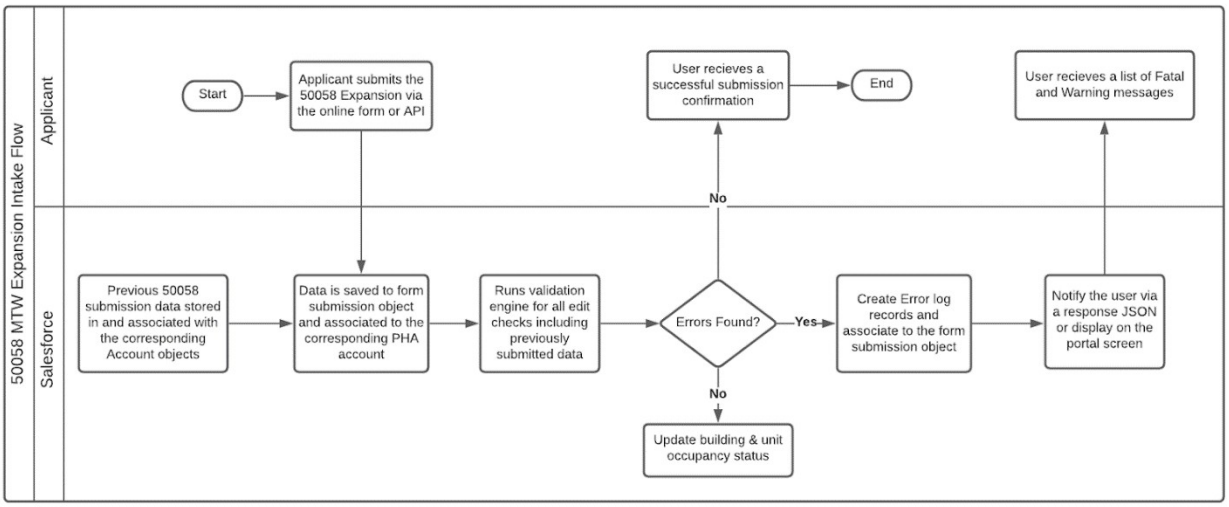
- User access, log in directly to the application: *Organization B* must submit a user request for all users who will need to directly access the application with a user login/ID. The request document will include the Rules of Behavior, which each requested user must agree to. Once submitted, a user account will be created for the user. The user will also need to agree to the Rules of Behavior when logging into the system, which is posted on the login screen of the application.
- System to system connection: After signing this ISA, *Organization B* will need to work with HUD to update *Organization B's system* to connect to the appropriate end point and to establish a system account/ID. *Organization B* will need to designate individuals that will be associated with the system account/ID and will be responsible for the use of the system account.

After the 50058 data is submitted, the MTW Expansion application will validate the data and provide the submission status and any errors back to the vendor, either via the MTW Expansion application or through the system connection.

The topological diagram and business process flow are shown below.



Topological Diagram: Connection to the MTW Application



Business Process Flow

5. SIGNATORY AUTHORITY

This ISA is valid for one (1) year after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Either party may terminate this agreement upon 30 days' advanced notice in writing or in the event of a security incident that necessitates an immediate response.

MTW Expansion Application

Matilda Chiu

System Owner

_____

(Signature Date)

(System B)

System Owner Name

Title

_____

(Signature Date)

Hun Kim

Chief Information Security Officer

_____

(Signature Date)

CISO Name

Chief Information Security Officer

_____

(Signature Date)

Christopher Webber

Chief Information Officer (Acting)

_____

(Signature Date)

CIO Name

Chief Information Officer

_____

(Signature Date)