	Georgia Technology Authority		
Title:	Enterprise Service Bus		
PSG Number:	GM-15-008	**Topical Area:**	
Document Type:	Guideline	**Pages:**	
Issue Date:	4/20/2015	**Effective or Revision Date:**	4/20/2015
POC for Changes:	GTA Enterprise Governance & Planning Division		
Synopsis:	Establishes guidelines for data sharing with sharing agreements		

PURPOSE:

Georgia Technology Authority's Data Sharing Services (DSS) operates an enterprise application known as the Enterprise Service Bus (ESB) which is used to share data among agencies. The ESB, a deployment of the webMethods middleware product suite for enterprise integration, is a central point of contact for software systems, databases and electronic files that are not able to communicate directly with each other. ESB can accept data in any format and in most programming languages convert the data to a consumable format and deliver the data to any host anywhere in any format needed. DSS meets the industry standard of 98.5% uptime for Web services.

The ESB and related services are designed to facilitate the creation of automated enterprise- wide information exchanges which can be uniformly developed, centrally maintained, quickly identified and discovered, and efficiently reused. The results include:

- Efficient and expansive information sharing between agencies,
- Cost-effective development and deployment of information systems, Improved operations,
- More timely, accurate, and complete information than possible through manual information exchanges, and
- Enhanced ability to meet local, state and federal reporting.

This guideline provides minimum requirements for an agency to use the ESB and outlines the criteria to establish an electronic interface.

SCOPE and AUTHORITY:

Information Technology Policies, Standards and Guidelines (PM-04-001) Data Sharing (PM-07-003)

GUIDELINES:

1. GTAs Data Sharing Service (DSS) responsibilities for the Enterprise Service Bus (ESB)

include the following:

a. Key participants: DSS Director and DSS Project Team.

b. Memorandum of Agreement (MOU) and Interconnection Security Agreement (ISA) signatory: State Chief Technology Officer, DSS Director, GTA security focal

c. Enrolling agencies to use the ESB. DSS meets with business, security and technical representatives of the potential provider of data and of the potential user(s) of data to determine their data sharing requirements, then, with approval of agency officials (i.e. business owners), initiates the data sharing project. There is no application form used to initiate ESB services. The formal authorization to initiate a project, a MOU that states each agencies' agreed responsibilities, is developed by DSS from a generalized template. When all pertinent processes and details are agreed to, the MOU is signed by appropriate officials. The agencies which are parties to the MOU are then considered to be Trusted Partners in the sharing situation described. The template MOU is included in Appendix I of this guideline.

d. Creating a Statement of Work which outlines the work tasks of the Trusted Partners and of DSS to implement a customer front-end to the ESB.

e. Document the technical and security specifications for the sharing situation covered by the MOU with an ISA. The ISA supports the MOU and is to be signed by officials of the DSS and Trusted Partners in the sharing situation described. A template ISA is included in Appendix II of this guideline.

f. Developing and testing the ESB technical and security capabilities described in the MOU and ISA.

g. Keep the ESB in working order, providing notice to Trusted Partners of any maintenance or interruption of service which may impact the operation of the ESB, and participating in testing to assure its operation following any interruption.

h. Include the ESB, as appropriate, in business continuity and disaster recovery plans and procedures, and ensure that these plans are tested according to State standards

2. The responsibilities of a potential provider of data and a potential user(s) of data relative to usage of the ESB are to collect or generate the following and make it available to DSS so that DSS can prepare the MOU and ISA:

a. Key participants:

i. Data provider data business owner, data steward and security focals (i.e. agency information security officer) and

ii. User data business owner, data steward and security focals,

b. MOU and ISA signators:

i. Data provider authorizing official, chief information officer and security focal,

ii. User data business owner, chief information officer and security focal,

c. Data within scope of the agreement include the following:

i. Impact categorization of the data based on FIPS 199 Security Categorizations,

ii. An agreed upon process to resolve data-sharing disputes,

iii. Statutory and regulatory restrictions impacting sharing or use of the data,

iv. Data security and data privacy constraints,

v. Responsibilities of the parties to the agreement for provision of data and for assurance of compliance with State and federal laws and regulations surrounding the data subject to the agreement.

vi. A listing of key contacts within the organization, such as key business stakeholders and data stewards.

vii. A listing of subject matter experts representing the organization who shall:

1. Identify their overall operational needs and requirements and provide on-site contact information,

2. Identify data access requirements, security requirements, (expected data volumes), growth estimates, data sharing partners and destinations,

3. Providing capacity planning requirements (trends, new requirements, etc.) on a quarterly basis.

3. Once an organization is accepted by GTA as a Trusted Partner in the ESB, the organization's responsibilities for implementing and operating with the ESB are as follows:

a. Creating interfaces and information sharing exchanges for producing or receiving data (i.e. the Trusted Partner's shared front end to the ESB), based upon the technical specifications published by GTA.

b. Ensuring that all data stewards are advised of GTAs security requirements and/or data sharing agreements, and ensure that the data stewards' established procedures comply with those requirements.

c. Participating in User Acceptance Testing by designating an owner and appropriate team members responsible for participating in design sessions, test case definition, testing and acceptance. Successful testing shall be indicated as follows:

4. GTA and the Trusted Partner shall jointly execute the test procedures to evaluate the effectiveness of the interface and to identify any vulnerability. DSS' testing capabilities include preparing test plans and test cases, and performing quality, black box, white box, regression, usability, availability, sanity, accessibility, regulatory and compliance, security, documentation, remediation, functional and non-functional testing. Results of testing shall be documented and appropriate corrective action taken, when the data providing and data receiving parties are satisfied that the interface is operating as

designed, the Trusted Partner officials (i.e. business owners) shall issue an authorization decision to operate.

5. The parties to the MOU need keep the providing and/or receiving shared front ends in working order, providing to DSS notice of any maintenance or interruption of service which may impact the operation of the ESB, and participating in testing to assure its operation following any interruption.

6. The parties to the MOU need to include the ESB, as appropriate, in business continuity plans and procedures, and ensure that these plans are tested according to State standards.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Enterprise Information Security Charter PS-08-005

Appropriate Use of Information Technology Resources PS-08-003

Appropriate Use and Monitoring SS-08-001

Data and Asset Categorization PS-08-012

Data Categorization – Impact Level SS-08-014

Information Security Management Organization SS-08-006

Information Security Risk Management PS-08-031

Integration Middleware SA-07-020

System Security Plans SS-08-028

Security Awareness Program PS-08-010

Security Education and Awareness SS-08-012

System Lifecycle Management SS-08-025

TERMS and DEFINITIONS:

Data – Any representation of facts, concepts or instructions (structured, semi-structured or unstructured) in a formalized manner suitable for communication, interpretation or processing by people or by machines.

Data Owner – The data owner is the agency responsible for creating, disseminating and/or maintaining specific data, and its accuracy and completeness. This entity shall be responsible for protecting and managing the use and sharing of the specific data and well as insuring the quality, usefulness and integrity of the interface.

Data Security - Safeguards for creation, modification, transportation, storage, and destruction of data.

Data Steward – The specific employee or position assigned by a Data Owner to protect and manage the use of specific data and data exchange interface. User or recipient agencies are responsible to the Data Owner and assigned Data Steward to conform to the protection and usages agreed upon based on the data's specific data classification.

Data sharing – Data sharing is allowing data to be used by an entity outside of the Data Owner's organization.

Enterprise Service Bus (ESB) – An enterprise-wide service that utilizes webMethods middleware that facilitates secure data sharing between authorized participants. ESB provides interoperability between systems/application shared front ends by rapidly establishing interconnecting interfaces to the middleware regardless of system/application type, age or complexity.

Shared Front End – A shared front end is a software interface that is used to exchange data between two or more business partners. This interface can exist at the Web tier, application tier or database tier depending on business requirements, on architecture, on design or on security constraints.

Trusted Partner – A Trusted Partner is an entity who negotiates an agreement with one or more other entities outlining minimum efforts, security controls and privacy protections to make information available. An entity shall not be entitled to be a Trusted Partner if it is unable to adhere to security controls and privacy requirements or fails to conform to the policies and procedures set forth in the agreement. In the State of Georgia ESB, a Trusted Partner may be any of the following entities:

1. A governmental entity of the State of Georgia (i.e., a state department, agency, board, bureau, commission, and authority, as well as an entity within the judicial or legislative branch of state government, or an entity within the University System of Georgia).

2. A Local Agency within the State of Georgia (i.e., political subdivisions of the State; or other entities created by the Constitution or laws of the State or created by local governments).

3. A private (for profit or non-profit) entity.

A Trusted Partner may be a data source, a data receiver or both by setting forth in a data sharing agreement to be bound by the principles, policies and procedures established in that agreement.

User Acceptance Testing (applied to a front-end interface) – User Acceptance Testing is a process intended to ensure the satisfaction of Trusted Partner expectations, usually by testing a representative sample of the functionality of the interface. At the completion of the testing, all Trusted Partners must be satisfied that the interface does indeed meet all their expectations, or alternatively, that they are willing to accept any deficiencies thereof.

Appendix I TEMPLATE

MEMORANDUM OF UNDERSTANDING FOR DATA SHARING

BETWEEN [Agency A], [Agency B], [Agency C]

BACKGROUND

WHEREAS, [Agency A], [Agency B], and [Agency C] are empowered to enter into this Agreement pursuant to 1983 Ga. Const. Art. IX, Sec. III, Para. I as an intergovernmental agreement.

WHEREAS [Agency A] has created a confidential and secure method for the transmission of [type of business data involved] between [Agency B and Agency C];

NOW THEREFORE, the purpose of this Memorandum of Understanding (MOU) is to create a working relationship between the [Agency A], [Agency B], and [Agency C] for the purpose of transmitting data required by [Agency C]. This MOU further serves to delineate the roles and responsibilities of the parties with respect to the confidentiality of such data.

PRIVACY AND SECURITY PROVISION

The parties acknowledge that the existence and applicability of [cite each governing agency, policy, guideline applicable]. Each party acknowledges their responsibility to abide by the terms of the applicable governing agency, policy, guideline with respect to the transmission and handling of [name type of business data in scope]. ["nnnn" data is provided by [Agency B] [list system name] to [Agency A] as required by and subsequently transmitted to [Agency C] [state whether is it by law, essential business need, etc.] will only be used for the limited purposes required by [cite the business need]. Any unauthorized release of [cite the business type] transmitted under the terms of this MOU shall immediately be reported to all parties.

[AGENCY A]

In addition to the provisions above, [Agency A] agrees to:

- [state the actions taken on data by Agency A].
- Maintain proper access and logging for any data used for this purpose.
- Not re-disclose any data or information to third parties.

No term or condition of this agreement shall prohibit [Agency A] from disclosing any other data or information pertinent to normal business operations under the rules and regulations as promulgated by [Agency A].

[AGENCY B]

In addition to the provisions above, [Agency B] agrees to:

- Provide [Agency A] with any pertinent data or information required by [Agency A] [cite system of record].

[AGENCY C]

In addition to the provisions above, [Agency C] agrees to:

- Provide a secure gateway for data transmission between [Agency A and Agency B].
- Not store or retain any data transmitted between the [Agency A and Agency B].
- Not access or allow any unauthorized access to data transmitted between [Agency A and Agency B].
- [Agency C] will provide the parties upon request with an audit trail of data transmissions between the [Agency A and Agency B] systems. [Agency C] will retain this audit trail for 3 years.

COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the data transmission. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

[Agency A] and [Agency B] agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection.

To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the parties agree to provide notice of specific events within the time frames indicated below:

Security Incidents: Technical staff will immediately notify their designated counterparts by telephone or e- mail when a security incident(s) is detected, so the other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).

Disasters and Other Contingencies: Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.

Material Changes to System Configuration: Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the ISA within one (1) month of implementation.

New Interconnections: The initiating party will notify the other party at least one (1) month before it connects its IT system with any other IT system, including systems that are owned and operated by third parties.

Personnel Changes: The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any

changes in point of contact information. Both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

INTERCONNECTION SECURITY AGREEMENT

The technical details of the systems interconnection (data transmission) will be documented in an Interconnection Security Agreement (ISA). The parties agree to work together to develop the ISA, which must be signed by both parties before the interconnection is activated.

Proposed changes to either system or the interconnecting medium will be reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before changes are implemented.

SECURITY

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA.

Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies.

PERIODIC REVIEW AND AMENDMENTS

The parties will evaluate progress of the MOU on an annual basis, and amend the MOU as appropriate. Amendments to the MOU shall become effective upon signature of all parties.

TERMINATION

The MOU may be terminated at any time upon written notification from either party to the others. Such notification must be provided fifteen calendar (15) business days prior to the termination. Provisions regarding security, confidentiality and [cite each governing agency, policy, guideline applicable] survive the termination of this agreement.

TERM

The MOU shall become effective upon the date of last signature, and shall remain in effect for a period of five (5) years. The MOU may be renewed at expiration upon signature of all parties.

Agreed upon and entered into by:

For [Agency A]

State Chief Technology Officer _____ Date _____

DSS Director _____ Date _____

GTA security focal _____ Date _____

For [Agency B]

Data Provider Authorizing Official _____ Date _____

Chief Information Officer _____ Date _____

security focal _____ Date _____

For [Agency C]

Data user business owner _____ Date _____

Chief Information Officer _____ Date _____

security focal _____ Date _____

Appendix II

TEMPLATE INTERCONNECTION SECURITY

AGREEMENT (ISA) FOR DATA SHARING

BETWEEN THE [Agency A], [Agency B] and [Agency C]

The requirements for interconnection between [Agency A], [Agency B] and [Agency C] are for the express purpose of exchanging data between [System Name], owned by [Agency B], and [System Name], owned by [Agency C] via the confidential and secure method for the transmission of data owned by [Agency A]. In this ISA, [Agency A], [Agency B] and [Agency C] may be referred to individually as "Party" or collectively as "Parties".

SECTION 2: SYSTEM SECURITY CONSIDERATIONS

General Information/Data Description. The interconnection owned by [Agency A] between [System Name], owned by [Agency B], and [System Name], owned by [Agency C] is a two- way path. The purpose of the interconnection is to deliver data to [Agency C].

Services Offered. No user services are offered. This connection only exchanges data between [Agency B]'s system and [Agency C]'s system via a dedicated in-house connection.

Data Sensitivity. The sensitivity of data exchanged between [Agency B] and [Agency C] is [State data sensitivity].

User Community. All [Agency C] users with access to the data received from [Agency B] are U.S. citizens with a valid and current [Agency C] 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 approved encryption mechanisms. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

Trusted Behavior Expectations. [Agency A's] and [Agency B's] and [Agency C's] systems and users are expected to provide protection to the data and systems subject to the interconnection 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 [Agency B]'s "XXX Policy", [Agency C]'s "YYY Policy" and the Georgia enterprise security policy PS-08-005 “Enterprise Information Security Charter”.

Incident Reporting. The Party discovering a security incident will report it in accordance with incident reporting procedures required by Georgia enterprise security standard SS-08-004 “Incident Response and Reporting”. In addition, the party shall report the incident to all Parties to this ISA.

Audit Trail Responsibilities. All 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 three (3) years.

SECTION 3: TOPOLOGICAL DRAWING (Insert a drawing here.)

SECTION 4: 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.

Agreed upon and entered into by:

For [Agency A]

State Chief Technology Officer _____ Date _____

DSS Director _____ Date _____

GTA security focal _____ Date _____

For [Agency B]

Data Provider Authorizing Official _____ Date _____

Chief Information Officer _____ Date _____

security focal _____ Date _____

For [Agency C]

Data user business owner _____ Date _____

Chief Information Officer _____ Date _____

security focal _____ Date _____