

HEALTH AND ENVIRONMENTAL DATA INTEGRATION
PROJECT FOR HOMELAND SECURITY

**MAINE TRADING PARTNER
AGREEMENT**

Overview – Data Exchanges for Health and Environmental Data Integration Project

This agreement is a voluntary agreement between the Maine Department of Health and Environmental Testing Laboratory (HETL) (*data provider*), and the New Hampshire Department of Environmental Services (NHDES) (*data consumer*), for the exchange of the following Data Flows:

- Laboratory Analytical Testing Results Data

The data exchange will take place via the Exchange Network Challenge Grant Project-Health and Environmental Data Integration for Homeland Security.

1. Purpose

The purpose of this Trading Partner Agreement (TPA) is to identify the activities that HETL and NHDES will undertake as partners in exchanging the Health and Environmental Data Integration Project Data Flows (HLS Project Data Flows).

This agreement does not supersede any the existing or future Performance Partnership agreements or memorandums of understanding between HETL and NHDES. It is intended to deal with the specifics of the Exchange Network flow.

2. Background

This project is part of a partnership formed as a result of an EPA EIN Challenge Grant with multiple states and EPA in order to allow Electronic Data Exchange of laboratory data collected during a Homeland Security Event. This complete project is referenced in the EPA Challenge Grant web site. See Attachment 1.

3. Partner Responsibilities

3.1. Data Exchange Mechanism and Schedule

The HLS Project Data Flows data exchange described in this document uses a one-way transfer of data, from the HETL's node to the NHDES's Web Service Requester (*or Node*). The exchange utilizes the HLS Common Toolkit to implement the data exchange. The Common Toolkit Host (there are two hosts – HETL and NHDES) will register at the Host's Local Toolkit Registry instance that the HLS Project Data Flows are available. The HETL will register at the Central Data Services Registry (if available) that the HLS Project Data Flows are available. The NHDES will discover through the HLS Common Toolkit that the HLS Project Data Flows are available and retrieve metadata to determine information about each data flow and the required parameters.

The NHDES will make use of HLS Project Data Flows Web Services to pull data from the HETL's Node.

The NHDES will pull data from the HETL as is necessary during non-business hours unless an emergency requires pulling data during normal business hours.

3.2. Data Elements, Content, and Coverage

Data Format and Compatibility:

In order to improve data interoperability among the Data Consumers and Data Providers, a suitable data format should be selected for all data flows. Under the Exchange Network, the approved data exchange format is XML. XML payload files should adhere to the recommendations of the Exchange Network. Employing Web-Services to exchange data within the project ensures that the project work may be used across multiple platforms.

In addition, the HLS Common Toolkit provides support to transform the XML data into HTML format, Excel CSV format, and GIS display; the Toolkit also supports the possibilities for adding additional formats in the future.

Leveraging Existing Assets:

The Homeland Security project will leverage the existing functionalities of the Data Provider Node in order to receive Data Service Requests, generate XML payload files, and transfer the XML payload files to the Data Consumer. Technologies that have been identified for reuse from the current capabilities of Maine and Exchange Network include:

1. Node
2. Shared Schema Components (SCCs) and Core Reference Model
3. Environmental Data Standards
4. NAAS security process
5. EDWR schema from the Exchange Network

User Account Establishment:

By default the HLS Common Toolkit will require a NAAS user account as a first level of data access restriction. An interface is provided through the application to request and receive NAAS accounts over the internet. Only Node administrators have access to this interface and a Data Consumer / Provider NAAS user accounts will need to be requested through an administrator.

If the NAAS option is not feasible for certain Data Consumers / Providers, private Node user account authentication may be used. Node administrators will also be responsible for maintaining user accounts and corresponding security rights if this option is chosen.

System Performance:

The data transfer process will allow Data Consumers in some cases to retrieve data directly from the Data Provider's production source database. In order to address concerns on data loading and to ensure that this process is transparent to the Data Provider, Data Services that may return a large volume of data can be implemented using a Node Solicit which will only use source database resources during off-peak hours as defined by the Data Provider. The Node Query data service method will only be implemented Data Services dealing with relatively small amounts of data.

In addition, to save data storage resources on application and database servers, a clean-up procedure may be implemented by the server administrators to remove data to be considered "out-of-date" or obsolete. System performance testing will be conducted before the application is moved to production.

3.3. Data Stewardship

The stewardship responsibilities of the trading partners are established and acknowledged by this agreement. The HETL will be a steward to all data on the HETL's regulated database systems for all HLS Project Data Flows.

Each partner will provide notification and documentation to the other partner when either decides that data quality, completeness or timeliness has fallen short of expectations.

The Homeland Security Project Implementation will adhere to a broader management process of data stewardship. Data stewardship includes the management systems and protocol of data ownership, quality, standards, security, reconciliation protocols, and asset management. The design approach includes:

1. The data sources for all Data Flows will continue to be managed and maintained by the current respective HETL authorities.
2. The Maine Node will continue to serve as the primary gateway for publishing and maintaining available Data Flows.
3. The HLS Common Toolkit will be used by the Data Consumers as a way to access the HETL Data Flows.
4. The EPA NAAS application will be used as the first level of user account authorization. If the NAAS option is not feasible for certain Data Consumers / Providers, private Node user account authentication will be used.

3.4. Data Confidentiality and Security

The system must ensure that all data exchanges are done in a safe, secure manner. Such standards / technologies as XML Encryption, XML Signature, XKMS, WS-Security, and XML Firewall are continuing to be investigated and evaluated.

Security will be maintained by each partner to adequately ensure the integrity and accuracy of the data. In order to address the concern for Data Confidentiality under the HLS Project, three levels of data classification have been developed to help examine the issue:

Level	Description
a. Public Info.	Data may already be available to the general public and/or will not incur unwanted consequences if made available to the general public.
b. Restricted	Data may contain sensitive personal or corporate information that should not be made available to the general public. However, non-public agencies with access to the Data Provider node will have complete access to this data.
c. Highly Confidential	Data is highly confidential and should be restricted to authorized personnel. Data should be restricted to a set of Data Consumers defined by the Data Providers.

Data Flow	Level	Data Sharing Practices	Design Approach
Drinking Water Lab Analytical Data (e-DWR)	Restricted	<p><u>Current process:</u></p> <ol style="list-style-type: none"> 1. Lab Analytical Data is considered somewhat sensitive and should not be made totally available to the public 2. Most of the lab data are made available to all internal staff via StarLIMS <p><u>“To-be” process:</u></p> <ol style="list-style-type: none"> 3. Data will be provided in a larger dataset through query 4. Data will be offered through web-services interface 	<p><u>Security Measures:</u></p> <ul style="list-style-type: none"> ▪ User account authentication will be accomplished by either (1) NAAS security verification, or (2) via Node user private account verification ▪ Trading Partner Agreement(s) may need to be implemented between the Data Provider and Data Consumer to ensure that the confidentiality of the Lab Analytical Data is maintained ▪ Data Element sharing will be pre-approved by the Data Providers during the Data Flow Implementation ▪ Access privileges will be fully controlled by the Data Providers

Table 1: Data Flow Confidentiality Analysis

The HETL has all rights to share this data with EPA or any other data exchange partner. The HETL can also make this data publicly accessible through the agency’s website unless the data is subject to any other confidentiality agreement.

For confidential data, the NHDES will need to gain permission from the HETL for using this data outside the agency and/or publishing this data via a website. Additional Trading Partner Agreements may be necessary to ensure the levels of Data Confidentiality and Integrity extend to any third-party agencies that may wish to obtain the data.

3.5. Standards and Technology

HETL and NHDES will exchange data using Web Services technology, which employs Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML).

In addition, the HLS Common Toolkit provides support to transform the XML data into HTML format, Excel CSV format, and GIS display; the Toolkit also supports the possibilities for adding additional formats in the future.

3.6. Data Source and Data Quality

The data exchange partners will cooperate to ensure that the data being exchanged is current, accurate and complete. Reconciliation of data duplicates, discrepancies, or other quality issues will be in accordance with the process outlined in the section Dispute Resolution.

3.7. Data Timeliness

The HETL will make the data for the HLS Project Data Flows available after the data has been sufficiently entered/updated into the HETL's regulated database system.

3.8. Dispute Resolution

If at any time one of the partners finds a problem with data quality or completeness, they should start the resolution procedures.

HETL and NHDES data administrators will resolve disputes whenever possible. (Data administrators are those assigned with the overall management of HLS Project Data Flows in his or her agency.) The data administrator will contact his or her counterpart, either by telephone, email, or in writing. If the data administrators cannot resolve the dispute within two weeks, they will bring it to the attention of their immediate supervisors.

4. Period of Agreement

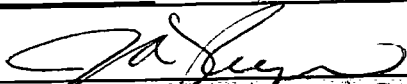
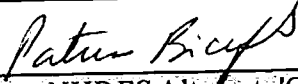
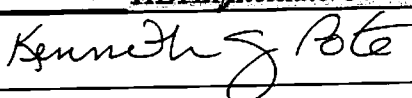

This Agreement becomes effective on the date of signatures by both parties and continues until modified by mutual consent or unless terminated with 60 days written notice by either party. Partners should review this agreement periodically, at least once per year. They should amend or revise it as changing needs, conditions or technology warrant.

5. Legal Framework – Disclaimer

This is a voluntary non-binding agreement between HETL and NHDES regarding the exchange of HLS Project Data Flows data. This agreement does not fulfill any specific legal requirements and participation does not supersede any data or information management and reporting requirements of any grant, contract, or other agreement.

6. Points of Contact / Signatures

The following individuals have been identified as points of contacts within each partner agency:

HETL Primary Contact	NHDES Primary Contact
	
HETL Alternate Contact	NHDES Alternate Contact
	

Attachment 1

The Department of Homeland Security recognized EPA's capabilities for preparing for and responding to national emergencies and therefore considered EPA's role crucial for planning the National Strategy. EPA released its Strategic Plan for Homeland Security in September 2002; in which it had identified the need for sharing environmental, health, and safety information.

The environmental state agencies of Michigan, Maine, New Hampshire, and New Jersey were awarded the exchange network grant for the year 2004 by EPA. Under this project, the States will design and implement homeland security data exchange to make available their environmental, health, and safety information to interested recipients including national security, law enforcement, first-responders, intelligence communities as well as the general public.

The purpose of this multi-state project is to improve the ability of the States to prevent, prepare for, and respond to events that threaten the nation's Homeland Security. This project will proceed in three stages:

1. Technology and Business Process Research: This stage will involve research and analysis of the existing infrastructure and security, and provide recommendations to the States to modify their infrastructure for the project implementation. This stage will also encapsulate the identification of data sources and data consumers for this project.
2. Infrastructure and Systems Design: The second stage of the project will be dedicated to designing the solution envisioned for this project. This will include designing the framework for integrating the health and environmental data including the data exchange mechanism, data exchange standards, and data flow configuration.
3. Implementation of the Homeland Security Data Exchange: The third stage of the project will involve implementing the data exchange mechanism that was designed in the second stage thereby allowing the States to integrate their environmental, health and safety data.

At a broad level, the Project developed technologies and tools to help states advance their capabilities to participate in the National Environmental Information Exchange Network (NEIEN). In order to achieve this broad goal, the project shall have the following objectives:

1. Provide states with ability to prepare for and respond to emergencies
2. Identify key data sources and potential data consumers
3. Streamline data exchange in order to provide quick and easy data access to first-responders and decision-makers
4. Implement a Homeland Security data flow for each State that includes Health, Environmental, and Safety information

The Exchange Network is a secure Internet- and standards-based approach for exchanging environmental data and improving environmental decisions. The U.S. Environmental Protection Agency, State environmental departments, and U.S. tribes and territories are partnering to build the Exchange Network to increase access to environmental data and make the exchange of data more efficient.

A Network Node is a web server that facilitates the interface between database systems and the Network. It is an entity's "point of presence" on the Exchange Network. Using standards-based web services and eXtensible Markup Language (XML) schema, Nodes securely initiate and respond to requests for information. With properly configured Nodes, Network trading partners can seamlessly exchange data regardless of hardware, operating system, or programming environment.

Nodes are defined by their specific function, rather than what they are in a physical hardware sense. Network participants may use several different hardware and software approaches and combinations to establish a Node. For example, a Network participant could implement a Node with: 1) specialized Node software on a dedicated server; 2) one or more types of software on more than one server; or 3) existing enterprise software on an existing server. Network partners are free to choose their own approach to Node establishment—what is important is that the Node performs its functions as outlined in the http://www.exchangenetwork.net/node/dev_toolbox/node_functional_spec_v1.1.pdf.

While this node function is to allow both requesting data from the Network, as well as publishing data to the Network in response to requests from other Network Nodes, alternatively the option does exist to be solely a Node client. Node Clients can submit, request, and receive data on the Network, but cannot respond to data queries from other Nodes.