Virtual USA Regional Information Sharing Memorandum of Agreement

SECTION 1. This document may be cited as the Virtual USA Regional Information Sharing Memorandum of Agreement (MOA) Version 1.2.

ARTICLE I - PURPOSE AND AUTHORITIES

This MOA is made and entered into by and between participating stakeholders, which enact this agreement, hereinafter called Members. The purpose of this MOA is to provide a governance framework for information sharing between the Members entering into this MOA and any Member designee, herein referred to as an authorized representative who participates in the information sharing or consumption of said information.

ARTICLE II - GENERAL IMPLEMENTATION

The prompt, full, and effective utilization of shared information among participating Members, including any information on hand or available from participating stakeholders or any other source, that are essential to the safety, care, and welfare of the people in the event of any incident affecting a party Member, shall be the underlying principle on which all articles of this MOA shall be understood.

Each party Member entering into this MOA recognizes the following:

- Many incidents transcend jurisdictional boundaries;
- Intergovernmental information sharing and coordination is essential in managing these and other incidents under this agreement;
- There will be incidents which require immediate access to information in another jurisdiction;
- Sharing information during incidents is critical to other Members' prevention, protection, response and recovery efforts; and
- There is a need for information to be timely and accurate.

On behalf of the authorizing body for each Member participating in the agreement, the authorized representative who is assigned responsibility for incident management will be responsible for formulation of the appropriate multi-jurisdictional prevention, protection, response and recovery procedures necessary to implement this MOA.

ARTICLE III - PARTY MEMBER RESPONSIBILITIES

It shall be the responsibility of each party Member to formulate internal procedural plans and programs for multi-jurisdictional prevention, protection, response and recovery activities to support the performance of the responsibilities listed in this article. In formulating such plans, and in carrying them out, the party Members, insofar as practical, shall acquire and develop information sharing capabilities (e.g., a centralized visualization tool, de-centralized information sharing practices, etc.) that best meet their needs and maintain reliable data sources.

A Member's authorized representative may request assistance of another Member's authorized representative by contacting them directly. The provisions of this agreement shall only apply to requests for information made by and to authorized representatives. Requests may be verbal or

in writing. If verbal, the request shall be confirmed in writing within 30 days of the verbal request. Requests shall provide a description of the information request and the point of contact.

ARTICLE IV - INFORMATION REQUIREMENTS

Information Sharing: Party Members agree to pre-identified types or categories of data layers to share from a pre-identified list of priority data sources as needed and as noted in the MOA appendices. Members agree that all information will only be shared using the information sharing structure provided by the U.S. Department of Homeland Security (DHS) as described in Article V and no copies of the source data will be posted or distributed in any form.

Information Assurance: Each Member will provide information assurance to verify that all shared data is derived from an authoritative data source (custodial owner). Members shall not directly contact another Member's data source, but will agree to work with the data coordinator (Member) for any follow-up required from the information provided. Members, insofar as practical, will provide data layers with the metadata requirements identified in the MOA appendices.

Requests for Information: Members, insofar as practical, agree to automate requests for information and handle such transactions between relevant members on a case-by-case basis.

ARTICLE V - ARCHITECTURE

Members will be responsible to develop their respective internal information sharing architectures needed to support information sharing between disparate Member visualization tools. Members will, within their respective architectures, identify and solve technical challenges that hinder or prevent the necessary sharing of information. At a minimum, Members agree upon an information sharing structure, how to share data files and analytical services, cyber security requirements and information protection standards for all participants as outlined hereafter.

Information Sharing Structure: Insofar as practical, Members shall agree to share information directly with other Members on the basis of the terms outlined in this MOA and/or provide access to each of their available data layers through the DHS-supplied information sharing structure described in the MOA appendices. Members will share information by granting access to the relevant data layer streams from their servers to other Members.

Data Files and Analytical Services: Insofar as practical, Members agree to use open-source standards and publish their data files in the pre-identified data file extensions identified in the MOA appendices. States will work toward producing a feed so that all Members may consume the information using a technology agnostic platform if technically feasible.

Cyber Security: Participants will adhere to baseline system security requirements for information to be shared across all jurisdictions. Member system security protocols will adhere to standard industry best practices.

Identity Management: Members will vet users through their own internal process wherein Member's information coordinators will sponsor individual participation and third party access

to information. Only Members' information coordinators will have access to the DHS-supplied information sharing structure.

Information Protection: Members will agree to only share information in accordance with its classification including, but not limited to, Protected Critical Infrastructure Information and law enforcement sensitive information. Members will agree to the roles and levels of security and data sensitivity that are used in the DHS-supplied information sharing structure identified in the MOA appendices.

ARTICLE VI - PERMISSIONS TO SHARE

Due to the sensitive nature of information shared relative to a multi-jurisdictional incident, Members agree to adhere to information sharing permissions, to the extent permitted by Members' freedom of information laws. Members must obtain the permission of the data provider prior to sharing information with non-Members. This may be performed on a case-by-case basis or through a memorandum of understanding.

ARTICLE VII - LIABILITY

Officers or employees of party Members rendering support or technical assistance to another Member pursuant to this MOA shall be considered agents of the requesting Member for tort liability and immunity purposes; and no party Member or its officers or employees rendering support or assistance to another Member pursuant to this MOA shall be liable on account of any act or omission in good faith on the part of such forces while so engaged. Good faith in this article shall not include willful misconduct, gross negligence, or recklessness.

Members will use any information or technical assistance provided by other Members at their own risk. Inasmuch as Members adhere to the information assurance process, no Members shall hold others liable and all Members acting in good faith will be indemnified from any liability claims to the extent permitted by the Member's laws, assuming also that the source will be responsible for the quality, accuracy, and scoring of their data.

ARTICLE VIII - IMPLEMENTATION

This MOA shall become operative immediately upon its endorsement by any two (2) Members; thereafter, this MOA shall become effective as to any other Member upon its endorsement. This document is for the sole benefit of the signatory parties, and no third party is intended to be a beneficiary thereof or have any rights as a consequence of this document. Any party Member may withdraw from this MOA, but no such withdrawal shall take effect until 30 days after the authorized representative of the withdrawing state has given notice in writing of such withdrawal to all other party Members. Such action shall not relieve the withdrawing Member from provisions assumed hereunder prior to the effective date of withdrawal.

Duly authenticated copies of this MOA and of such supplementary agreements as may be entered into shall, at the time of their approval, be deposited with each of the party Members and with the Department of Homeland Security and other appropriate agencies of the United States Government.

ARTICLE IX - VALIDITY

This MOA shall be construed to effectuate the purposes stated in Article I hereof. If any provision of this MOA is declared unconstitutional, or the applicability thereof to any person or circumstances is held invalid, the constitutionality of the remainder of this MOA and the applicability thereof to other persons and circumstances shall not be affected thereby.

APPENDIX - Virtual USA Regional Information Sharing Memorandum of Agreement

The Virtual USA Regional Information Sharing MOA appendix serves as a living document designed to reflect the current state of agreement based upon the technological, governance and operational capabilities of the Members.

I. Information Sharing Guidance

Participating Members identified the following regional information sharing principles and guidelines:

A. File format – Members agree to share files in Keyhole Markup Language (KML), Compressed Keyhole Markup Language (KMZ), Web Map Service Interface Standard (WMS), Geographically Enabled Really Simple Syndication (GeoRSS), Extensible Markup Language (XML) or Representational State Transfer (REST) formats.

   a. XML - is a set of rules for encoding documents in machine-readable form.
   b. KML - is an XML language focused on geographic visualization, including annotation of maps and images.
   c. KMZ - consists of a main KML file and zero or more supporting files that are packaged using a Zip utility into one unit, called an archive. The KMZ file can then be stored and shared/accessed as a single entity.
   d. GeoRSS - is a family of web feed formats used to publish frequently updated content (in this case, geographically referenced content). There are currently two encodings of GeoRSS: GeoRSS Simple and GeoRSS Geography Markup Language (GML), which is an XML grammar for expressing geographical features.
   e. WMS - provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases.
   f. REST Services - supports various formats, including: KML, HTML, LYR (layer file), NMF (ArcGIS Explorer map file), JSAPI (JavaScript), VE (Virtual Earth), and GMaps (Google Maps).

B. Metadata – Members agree to provide data layers with the following metadata requirements:
   1. Data Source – originator
   2. Type of data – description, abstract and purpose
   3. How often updated – maintenance and update frequency
      a. Periodicity or “as needed”
   4. Data coordinator – point of contact
   5. Published Access to Information – URL, etc.

C. Roles – Members agree to categorize user groups according to the following roles: Contractor, Security, Emergency Response, and Executive.

D. Priority Indicators and Status Variables – Members have identified priority indicators, categories of information, and status variables (figure 1) that they have deemed important to share regionally with other relevant Members, when appropriate, based upon operational needs as determined by each Member. When sharing information designated as a priority indicator, members will designate that information accordingly by selecting the “priority” button when uploading/sharing the web link through the vUSA

environment (currently the Generation II Prototype). The regional priority indicators and status variables identified in May 2010 are as follows:

1. County/Parish Emergency Operations Center Status
2. Local State of Emergency Status
3. Evacuation Status
4. Shelter Capacity Status
5. Schools Status
6. Electrical Power Status
7. Water Status
8. Communications Status
9. Debris Status
10. Major Highways Status
11. Emergency Services Status
12. Search and Rescue Status
13. Medical/Health Status
14. Re-entry: Post Evacuation Status
15. Major Retailer Operations Status
16. Emergency Fuel Supplies Status
17. Gas Stations Status
18. Generating Capacity Status

Regional Priority Indicators	Red	Yellow	Green
County/Parish EOC Status			
Status	*Level 1 – Full activation*	*Level 2 – Partial activation*	*Level 3 – Operational/ Monitoring*
Local State of Emergency			
Status	*Declared*	*Previously declared, now rescinded*	*None*
Evacuation			
Status	*Mandatory*	*Voluntary / Phased*	*None*
Shelter Capacity			
Status	*Less than 50% capacity remaining*	*More than 50% capacity remaining*	*Closed*
Schools			
Status	*Closed*	*District open, some schools closed*	*Open*
Electrical Power			
Status	*Less than 80%*	*Between 80% and 90%*	*More than 95%*
Water			
Status	*No water / Low pressure*	*Boil water notice*	*Operational*
Communication			
Status	*Emergency communication failed or limited*	*Emergency communication up, commercial failed or limited, including cellular*	*Normal operations*
Debris			
Status	*Emergency debris clearance*	*Emergency debris removal*	*Debris management plan implemented and/or normal operations*
Major Highways			
Status	*Closed*	*Limited use /Emergency use only*	*Open*
Emergency Services			
Status	*Mutual aid required*	*Emergency staffing plans implemented*	*Normal operations*

Search and Rescue			
Status	*Primary search required / Ongoing OR Search required/limited or no resources available*	*Secondary required / Ongoing OR Search required/ongoing*	*All clear*
Medical / Health			
Status	*DMAT required / On scene*	*Limited services / DMAT not required / Released*	*Normal operations*
Re-entry – Post Evacuation			
Status	*No entry*	*Qualifiers – No electrical, water, limited time, etc.*	*No restrictions*
Major Retailer Operations			
Status	*Stores closed*	*Stores open / Limited operations or supplies*	*Stores open*
Emergency Fuel Supplies			
Status	*1-2 days supplies on hand*	*3-7 days supplies on hand*	*8+ days supplies on hand*
Gas Stations			
Status	*Widespread closures of gas stations*	*Limited fuel / Isolated station out of fuel*	*Normal operations*
Generating Capacity (power generating capacity within a state)			
Status	*Generating capacity emergency*	*Generating capacity alert*	*Generating capacity advisory / Normal operations*

Figure 1

E. Virtual USA Information Sharing Environment

The Virtual USA (vUSA) information sharing environment, also currently known as the Generation II Prototype, is web-based and has four common layers and one administrative layer: (1) a data registration, search, discovery, and alert system (search server); (2) a data download and exchange engine (exchange server); (3) a viewer layer; (4) a collaboration forum; and (5) an administrative layer for managing the environment's use and access.

The search server addresses the on-line catalogs of participating Members, polling each catalog constantly or at short intervals to detect new data offerings and send notifications based on a user's preferences. Each Member will register with the search server, which defines user groups by roles (Contractor, Security, Emergency Response, and Executive). Individual users register under one of the aforementioned roles and are approved by their

state administrator. Once registered, users will customize their participation by configuring their catalog view ("My Library") and requested notifications. Notification settings allow a user to passively search and receive a notification based on user-specified criteria, which include: general data domains or data types (such as alerts for creation of new EOCs), particular Members, geographical areas, or specified keywords. Users are also given the option to select their preferred notification method (e-mail or text message). Users logged onto the system are able to adjust their individual preferences at will, allowing them to customize the vUSA environment to support and meet their needs in a dynamic environment.

The system constantly polls the various catalogs, listening for any feeds that are available at a given time. During polling, the system queries the participating systems for a number of attributes or descriptors based on common elements, such as date/time posted, keywords, data domain types, and role relevance types. Based on protocols and user preferences, the search server sends notifications as required based on roles and individual preferences. It will also allow system administrators to broadcast alerts and messages to specified groups.

The prototype search server is built around GeoFinder for the Environment (GFE). GFE is a federated search tool capable of interfacing on command with multiple catalogs across users on the prototype. The Generation II Prototype expands the functionality of GFE by integrating open source tools with the required polling, registration, and alert capabilities, always using Open Geospatial Consortium (OGC) standards to the extent possible and as appropriate.

The data download and exchange server allows users to share web links to locally-held data, and to label that link with the required metadata as defined in the information sharing guidance section above. The exchange server allows users to view information being shared through a web link on one of the prototype's viewers, or to copy the link directly into their native system for usage in an operational environment. Additionally, the exchange server allows users to upload files to the prototype should they so choose. An example of a case when a user would wish to *upload a file* rather than *share a web link* is when the demands on a user *sharing a web link* compromise the bandwidth of a user's infrastructure, such as in the case of a large imagery file depicting an affected area. Therefore if the user chooses to do so, these large files can be uploaded, and hence viewed on a viewer within the prototype or downloaded to a user's native environment.

The Generation II Prototype provides a selection of viewers to allow users to visualize information at will and as needed. Both ESRI (Adobe Flex) and Google viewers will be available, so that the myriad of capabilities resident in both platforms can be leveraged. As more visualization tools become available (i.e., Bing Maps), users may identify those as new requirements and the tools will then be evaluated for integration into the prototype. Most importantly, this multi-viewer approach will enable users to work within the environment that they are most familiar and comfortable with.

vUSA's Generation II Prototype also provides a forum for users to collaborate and share best practices, lessons learned, and technical innovations that pertain to information

sharing initiatives. The forum also provides a place for users to request information from each other, and to work together on data development, share code, and collaborate on data management. The forum was designed to be flexible enough to allow the practitioners to collaborate in a rapidly changing environment where their needs and requirements may change unexpectedly.

The prototype's administrative layer allows designated users, herein referred to as "admins", to perform the management and administrative functions of their respective entity, whereas entity is defined as a state, federal or private organization designated access by the signatory to this core MOA. Through the administrative layer, "admins" can: (1) establish user accounts within their respective entity; (2) assign roles to users; (3) modify the content of the interface for users within their respective entity; and (4) designate other users within their entity as "admins" as well. This layer's functionality is important because it allows each entity to maintain its sovereignty and govern itself within the vUSA environment.

As the number of entities with access to the vUSA environment expands, the architecture will have to expand accordingly. Based on load testing data, more "prototype-like" systems will be fielded in a linear fashion in order to support the expanding community. These platforms will all be load balanced with each other in order to provide a seamless, redundant, and resilient capability for all users.

****

This appendix was last amended on July 7, 2010.
For more information about Virtual USA, please visit www.firstresponder.gov/virtualusa.

VIRTUAL USA

Developed by the U.S. Department of Homeland Security's Command, Control and Interoperability Division in partnership with the response community, Virtual USA creates a cost-effective nationwide capability to significantly improve information sharing and decision making during emergencies and day-to-day operations.