



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 2

[List View](#)**General Information** [Contact](#) [Default Values](#) [Discount](#) [Document Information](#) [Clarification Request](#)

Procurement Folder: 970413

Procurement Type: Central Contract - Fixed Amt

Vendor ID: VS0000016546

Legal Name: BUFFALO COMPUTER GRAPHICS INC

Alias/DBA:

Total Bid: \$643,506.78

Response Date: 12/21/2021

Response Time: 12:43

Responded By User ID: Buffalo8668

First Name: PATRICK

Last Name: CERRA

Email: rfpteam@bcgeng.com

Phone: 7168228668

SO Doc Code: CRFQ

SO Dept: 0606

SO Doc ID: HSE2200000005

Published Date: 12/10/21

Close Date: 12/21/21

Close Time: 13:30

Status: Closed

Solicitation Description: Emergency Management Information System (EMIS)

Total of Header Attachments: 2

Total of All Attachments: 2



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**State of West Virginia
 Solicitation Response**

Proc Folder: 970413
Solicitation Description: Emergency Management Information System (EMIS)
Proc Type: Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2021-12-21 13:30	SR 0606 ESR12212100000003830	1

VENDOR
 VS0000016546
 BUFFALO COMPUTER GRAPHICS INC

Solicitation Number: CRFQ 0606 HSE2200000005
Total Bid: 643506.7800000000279396772384 **Response Date:** 2021-12-21 **Response Time:** 12:43:30
Comments: Thank you for the opportunity to participate in this CRFQ process. BCG looks forward to the opportunity to demonstrate our capabilities.

FOR INFORMATION CONTACT THE BUYER
 David H Pauline
 304-558-0067
 david.h.pauline@wv.gov

Vendor Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Annual Subscription for EMIS - Initial Year	1.00000	EA	263021.010000	263021.01

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

- 4.1.2 Contract Item 1: Annual Subscription for EMIS Solution
- 4.1.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.
- 4.1.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Annual Subscription for EMIS - Optional Year 2	1.00000	EA	126828.590000	126828.59

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

- 4.1.2 Contract Item 1: Annual Subscription for EMIS Solution
- 4.1.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.
- 4.1.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Annual Subscription for EMIS - Optional Year 3	1.00000	EA	126828.590000	126828.59

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

- 4.1.2 Contract Item 1: Annual Subscription for EMIS Solution
- 4.1.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.
- 4.1.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Annual Subscription for EMIS - Optional Year 4	1.00000	EA	126828.590000	126828.59

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

4.1.2 Contract Item 1: Annual Subscription for EMIS Solution

4.1.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.

4.1.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per



Emergency Management Information System

WV DHS Emergency Management Division

CRFQ 0606 HSE2200000005

Due 12/21/2021

Prepared for:

David H. Pauline

Dept. of Administration, Purchasing
Division

2019 Washington St E

(304) 558-0067

david.h.pauline@wv.gov

Prepared by:

Patrick Cerra

Buffalo Computer Graphics, Inc.

4185 Bayview Road

Blasdell, NY 14219-2732

716-822-8668

rfpteam@bcgeng.com

CONTENTS

- SOLICITATION DOCUMENT5
- ADDENDUMS7
- EXECUTIVE SUMMARY8
- 3. QUALIFICATIONS 10
- 4. GENERAL REQUIREMENTS 19
- 11. MISCELLANEOUS..... 88
 - 11.1 Contract Manager..... 88
 - 11.2 Software as a Service Addendum 88
- APPENDIX A..... 99

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: BUFFALO COMPUTER GRAPHICS, Inc.

Name of Agency: West Virginia Emergency Management Division

Agency/public jurisdiction's required information:

- 1. Will restricted information be processed by the service provider?
Yes
No
- 2. If yes to #1, does the restricted information include personal data?
Yes
No
- 3. If yes to #1, does the restricted information include non-public data?
Yes
No
- 4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes
No

5. Provide name and email address for the Department privacy officer:
 Name: PATRICK LUPIANI
 Email address: PLUPIANI@bcgeng.com

Vendor/Service Provider's required information:

- 6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:
 Name: PATRICK LUPIANI
 Email address: PLUPIANI@bcgeng.com
 Phone Number: 716 822 8668

..... 99

EXHIBIT A – PRICING 100

SIGNED PURCHASING AFFIDAVIT 101

SAMPLE BCG MASTER SERVICES AGREEMENT 103



SOLICITATION DOCUMENT



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Quote

Proc Folder: 970413			Reason for Modification:
Doc Description: Emergency Management Information System (EMIS)			
Proc Type: Central Contract - Fixed Amt			
Date Issued	Solicitation Closes	Solicitation No	Version
2021-11-24	2021-12-14 13:30	CRFQ 0606 HSE2200000005	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code: VS0000016546
Vendor Name: BUFFALO Computer Graphics, Inc.
Address: 4185 Bayview Road
Street:
City: BLASDELL
State: NY **Country:** US **Zip:** 14219
Principal Contact: Patrick CERRA
Vendor Contact Phone: 716 822 8668 **Extension:** 103

FOR INFORMATION CONTACT THE BUYER

David H Pauline
 304-558-0067
 david.h.pauline@wv.gov

Vendor Signature X *Gay A. Masterson* **FEIN#** 161190997 **DATE** 3-Dec-2021

All offers subject to all terms and conditions contained in this solicitation

ADDENDUMS

Signed addendums list

ADDENDUM ACKNOWLEDGEMENT FORM SOLICITATION NO.:

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | | | |
|-------------------------------------|----------------|--------------------------|-----------------|
| <input checked="" type="checkbox"/> | Addendum No. 1 | <input type="checkbox"/> | Addendum No. 6 |
| <input checked="" type="checkbox"/> | Addendum No. 2 | <input type="checkbox"/> | Addendum No. 7 |
| <input type="checkbox"/> | Addendum No. 3 | <input type="checkbox"/> | Addendum No. 8 |
| <input type="checkbox"/> | Addendum No. 4 | <input type="checkbox"/> | Addendum No. 9 |
| <input type="checkbox"/> | Addendum No. 5 | <input type="checkbox"/> | Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Buffalo Computer Graphics, Inc
Company

David Masterson
Authorized Signature

3-Dec-2021
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

EXECUTIVE SUMMARY

RFP Subject: Emergency Management Information System

Number: CRFQ 0606 HSE2200000005

Vendor's Name: Buffalo Computer Graphics, Inc.

Business Address: 4185 Bayview Road, Blasdell, NY 14219

Phone: 716-822-8668

Fax: 716-822-2730

Contact: Patrick Cerra

Email: rfpteam@bcgeng.com

Buffalo Computer Graphics, Inc. (BCG) appreciates the opportunity to respond to West Virginia Emergency Management Division's (VWEMD) request for proposal for a web-based statewide EMIS enterprise solution.

BCG is privileged to have provided emergency management focused software solutions for American and Canadian governments and private entities for nineteen years, and maritime training, simulation, and communication software and hardware for thirty-nine years. We are experts with the requirements and technology landscape of emergency management agencies and departments and believe that we can provide a tailored configurable-off-the-shelf software solution that meets and exceeds the needs of VWEMD and its stakeholders involved with the State's EMIS platform.

BCG's proposal includes a configurable software solution based on its COTS DisasterLAN (DLAN) emergency management information system cloud-based software platform that can serve as a central emergency response platform and EMIS software system with scalable state-wide coverage. This solution will accommodate all VWEMD's projected users including VWEMD System Administrators, State Agency Representatives, Local Jurisdiction Representatives, Non-Governmental Organizations, Federal Agency Representatives, and other EMIS participants in terms of both scalability and feature sets designed for multi-agency collaboration. The DLAN system facilitates both day-to-day and emergency incidents by providing a modern web-based software solution with mobile applications.

BCG's DLAN products have already been successfully implemented for multiple State Agencies in the USA and Provincial Agencies in Canada. As a current example, BCG implemented a solution for the State of Oregon Department of Human Services in 2021 with an expedited timeframe. The success of this project has already led to an additional expansion to expand the solution with additional products and services for sheltering and refugee services management. In BCG's home state of New York, the New York State Department of Homeland Security & Emergency Service currently uses BCG's software as part of their NY-Responds statewide emergency management system, which can be accessed by all 62 New York State Counties as part of the State-wide implementation. The DLAN system is also utilized by all NYS Functional Groups, State Agencies, New York State Division of Military and Naval Affairs (National Guard), and many other stakeholders and organizations. BCG believes a similar model and implementation methodology would be successful for the State of West Virginia.

As a well-established provider of EMIS systems, BCG can provide a smooth fast implementation process to get customers up and running quickly. To achieve this end, BCG will work with Infinite One Technology Solutions, a long-time support partner who provides project oversight, coordination, and implementation services. BCG the

prime vendor. BCG agrees that it is able to implement the software within four months of final contract signing as per Addendum #2's additional mandatory requirement.

BCG is a company that is committed to excellence in emergency and incident management. The company requires that all employees that work on DLAN train in FEMA's ICS courses. Additionally, BCG's core management and many engineer staff come from emergency management or firefighting backgrounds. BCG can provide trained ICS staff and IMAT teams to supplement VWEMD's EMIS during a response. BCG understands the Emergency Operation Center environment, field response, planning, and executive decision making better than other software vendors, because we are emergency managers ourselves. This knowledge shines through in DLAN's thoughtful design, its ability to digitize key processes, and its multi-agency ready feature set. The system allows users to not just capture information for situational awareness and accountability, but to operationalize it in a meaningful way for effective decision making, prioritization, and task completion.

Thank you for the opportunity to present our DLAN system in our response to this RFP which we believe will successfully address VWEMD's mission to support statewide use by state agencies, local governments, regional and national partners, and private response partners throughout both day-to-day use and all areas of homeland security and emergency management.

Sincerely,



Patrick J. Cerra
Proposal Manager, BCG
21 December 2021

3. QUALIFICATIONS

Vendor, or Vendor’s staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1 Vendor shall provide a minimum of five (5) relevant reference to demonstrate that it has proven experience in managing hosted/on-premises Solutions at a statewide level. All referenced Solutions shall be currently operational in a production environment. This information shall be provided prior to contract award.

Reference #1 Oregon Department of Human Services

Oregon Department of Human Services (ODHS) – Emergency Management			
Contact Person:	Steve Pegram, Executive Director		
Contact’s Email:	Steve.s.pegram@dhsosha.state.or.us		
Address:	500 Summer St NE, E-15, Salem, OR 97301		
Contact’s Phone:	503-366-3934	Date of Service:	8/17/21-Present
Modules:	This is a DLAN Premium system with the following modules: Bed Tracking, Finance, GIS Premium, HICS Forms & Job Action Sheets, Special Needs Module, Chat, Communication Center, GIS, Incident Folders, Mobile Responder, Phonebook, Phonebook Premium, Reference Library, Resource Database, Social Media Basic, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Healthcare Industry Pack, ICS or IMS Forms Module, Incident Action Plan Module, Role Checklist Module, Situation Report Module, Damage Assessment Form, Report, & Board, Road Closure Form, Report, & Board, Role/Task Status Report & Board, Shelter Management Form, Report, & Board, and the Sheltering Module		
Scope of Work:	<p>Summary: This is a BCG cloud hosted 4-year contract. The system includes the DLAN Premium Edition with the Emergency Management Pack, Healthcare Pack, Finance Module & GIS Premium. The Oregon Department of Human Services (ODHS) is a state-wide agency with purview daily citizen services and programs as well as long-term risks and impacts from emergency and public health events. ODHS particularly focuses on critical human services such as short-term housing, sheltering, COVID-19 assistance, and supporting vulnerable populations.</p> <p>Details: In 2020 the State of Oregon recognized that short term and long-term impacts from the global pandemic required additional support and services from the State. A new emergency management team was created under the Department of Human Services to address coordination, planning, awareness, and services to Oregonians impacted by emergencies.</p> <p>ODHS implemented the DLAN software system in an expedited time frame. ODHS and BCG worked to design and deploy a system of dashboards based on FEMA’s Lifelines. This capability has allowed ODHS to collect situational information updates and essential</p>		

	elements of information from teams, departments, and facilities across the state. In addition to lifelines, ODHS and BCG implemented significant shelter staff management tools using the DLAN Mobile Responder App. A substantial expansion to ODHS' sheltering is planned for early 2022 focusing on family reunification, staff tracking, and other elements of long term sheltering.
--	--

Reference #2 Province of Ontario, Office of the Fire Marshal and Emergency (OFMEM)

Ontario Office of the Fire Marshal and Emergency Management (OFMEM)			
Contact Person:	Danylo Zakydalsky, Emergency Management Operations Officer		
Contact's Email:	Danylo.zakydalsky@ontario.ca		
Address:	Ontario Office of the Fire Marshal and Emergency Management (OFMEM) 25 Morton Shulman Ave, 5th Floor ,Toronto, Ontario M3M 0B1 Canada		
Contact's Phone:	647-329-1062	Date of Service:	2019 - Present
Modules:	This is a custom designed DLAN system. Modules include: Asset Management, Chat, Communication Center, finance Module, GIS Premium, IAPs, Incident Folders, Mobile Responder, Phonebook, Reference Library, Resource database, Situation Reports, Social Media Premium, Status Board Builder, Ticket Manager Premium, Additional Training Site.		
Scope of Work:	<p>Summary: DLAN enables the Province of Ontario to improve the input of necessary information to better support the monitoring, oversight, response and recovery to incidents that occur in vast Ontario communities and within the Ontario Public Service (OPS) organization. After a rigorous procurement process, Buffalo Computer Graphics (DLAN software) was selected by the Province.</p> <p>The DLAN software greatly enhances overall Provincial situational awareness during incidents, facilitates resource requests between stakeholders, assists in debris management and disaster assessments and streamlines emergency communications. Access to the system, which is also available on mobile devices, is being provided to emergency management officials within numerous provincial ministries, federal departments, municipalities, First Nations communities and select industry partners.</p> <p>Details: The robust DLAN software solution they have chosen supports all aspects of the Ontario Incident Management System (IMS). IMS serves as a framework in DLAN that guides organizational structures, functions, processes, and terminology. In addition to this, DLAN also includes standardized IMS values, forms, and fields in all areas of the system. DLAN exceeds other software solutions by taking these aspects and standardized values from IMS and using them to build out supportive processes, workflows, and response modules that work hand in hand to support technical and functional interoperability for both planned and unplanned events in Ontario.</p> <p>DLAN encourages an IMS based process for Ontario's handling information in the system at the following levels:</p> <p><i>User Level:</i> Each end-user has a clearly defined role/position in DLAN and receives tickets and messages tasked to his or her specific role that need to be managed or acknowledged. Role specific dashboards, homepages, and reports make information management and</p>		

	<p>interacting with the system quick and simple. Users pass information along to the next relevant role or person in the chain and all interactions are automatically logged. This helps maintain span of control and accountability for upper management.</p> <p><i>Section Level:</i> DLAN supports Ontario’s Dynamic Organizational Structures based on IMS standards. Each active IMS section (ex: Logistics, Operations, Planning, Fin/Admin, and Command) has access to specific software features designed to assist that section in performing their duties in response to the incident or event.</p> <p><i>Command Level:</i> Standardized and completely customizable reports in DLAN are available to command staff so that they can make timely decisions based on current information. For example, an Incident Commander or Executive dashboard may incorporate a ticket report showing life safety issues, a critical decisions list, an annotated GIS map of the incident area and affected infrastructure, and a curated social media stream of reliable source information.</p> <p><i>Multi-Agency and Multi-Jurisdictional Coordination Level:</i> DLAN supports Ontario’s coordinated communication and information sharing via standardized methods such as the ability to Email or forward documents and content out from the DLAN system to designated partners and other jurisdictions.</p> <p>For the ultimate coordination of Ontario’s emergency information, DLAN’s Ticket Sync feature allows real-time data synchronization between entities using their own DLAN software system in the region. OFMEM can directly exchange data with the City of Toronto OEM, City of Mississauga OEM, Halton Regional EOC, Toronto Hydro ESL, EMCT (Ontario Ministry of Health MOHLTC and LHINS), and neighboring cross-border entities such as New York State and Erie County, NY. OFMEM has the ability to send and receive critical information reports and resource requests including the ability to see comments and updates from ticket sync partners in real-time further enhancing a regional approach to incident management.</p>
--	--

Reference #3 NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)

New York State Department of Homeland Security and Emergency Management			
Contact Person:	David Smith, Operations Section Chief		
Contact’s Email:	david.smith3@dhses.ny.gov		
Address:	NYS Office of Homeland Security & Emergency Management 1220 Washington Avenue State Office Campus Building 22 Albany, NY 12242 United States		
Contact’s Phone:	518-292-5955	Date of Service:	2004 - Present
Modules:	This is a DLAN Premium system. Modules include: Chat, Communication Center, GIS Basic, Incident Folders, Mobile Responder, Phone Book, Phonebook Premium, Reference Library, Resource Database, Social Media, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Emergency Management Industry Pack,		

	ICS, IAP, Role Check list, Situation Reports, Damage Assessment, Weather, Separate Training Site, Watch Command
Scope of Work:	<p>Summary: The State of New York has branded their uniquely configured DLAN system as “New York Responds” for use within their State. They employ a full featured On Premise DLAN Enterprise solution with the addition of Ticket Manager Premium, Role Activity Log, Watch Command, Asset Tracking, Chat, GIS Premium, Training Site, and Watch Command Modules. Renamed as NY-Responds for the state of NY, the system is designed to be used by any county or state agency throughout NYS.</p> <p>Three days prior to the start of the Republican National Convention (RNC) in Madison Square Garden New York City, the director of DHSES called BCG with a statement that DHSES’s home-brewed EMIS had failed and that they had chosen DLAN from among 20 other systems as its replacement. They needed DLAN installed and running immediately. To meet this request, BCG staff travelled to DHSES, installed the system overnight, and spent Sunday testing and training core staff. Just-in-time training was provided to end-users and the system was used successfully throughout the RNC with people logged in from Albany, NY, New York City, Madison Square Garden event center, and New Jersey to manage the event. Over the long duration of its use at the NYS’s DHSES state-level emergency operations center, DLAN has transitioned from an early Version 3.1 to the current Version 12.x and has adapted to meet the mission critical resource requesting and tracking needs for NYS. Ongoing development work for DHSES over the years has helped BCG staff develop the skills necessary to design, build, and implement systems suited for statewide, multi-jurisdictional needs and deliver them on time and within budget. Recently, NYS has re-implemented the NY Responds system, of which BCG software is a key component. This unique statewide system allows all 62 counties to utilize one unified, feature-rich incident management solution. BCG has worked closely with the State to ensure the success of this ambitious project.</p> <p>Details: New York State has an extended support and maintenance package with BCG. In addition to our typical Platinum Plus Support plan, DHSES has added dedicated blocks of time to support their agency in a number of ways during daily usage, training, exercises, and EOC activations. Since BCG is intimately involved in the State’s workflows and procedures, the agency has also elected to have stand by contracting in place for onsite work that can be leveraged during trainings, exercises, and EOC activations in order to ensure that they have the vendor support they need to provide services like just-in-time training, workflow training specific to a user’s role, new feature training as upgrades come out, and support for onsite meetings for proposed features. In addition, the State has such confidence in BCG staff that they elected to include hours for BCG to support them in diagnosing non-DLAN issues such as client, server, and network problems that may impact their users. With BCG actively involved onsite in EOC activities, our staff is often able to diagnose an issue more quickly than external IT staff, allowing their staff to relay issues to IT more efficiently. Finally, in large activations like Hurricanes Irene and Sandy, the State has contracted with BCG to provide around-the clock 24/7 support within the EOC to assist them with both on-site troubleshooting and training during these large activations.</p>

Reference #4 New York Power Authority (NYPA)

New York Power Authority (NYPA)

Contact Person:	Joseph Flick, Director of Emergency Management		
Contact's Email:	joseph.flick@NYPA.gov		
Address:	123 Main Street, Mail Stop 10- H, White Plains, NY 10601		
Contact's Phone:	914-390-8095	Date of Service:	2017-Present
Modules:	DLAN Advanced with: GIS Premium, Phonebook Premium, Role Activity Log, Situation Reports, Status Board Builder, Ticket Manager Premium, Training Site, Weather		
Scope of Work:	<p>Summary: Although the original DLAN system was installed for NYPA in 2017, their use of the multi-featured software continues to grow and evolve to meet the changing needs of the organization. In addition to ramping up to meet any emergency situations that arise, the system is used in a day to day capacity to send and monitor Incident Notifications and to provide Situational Awareness from inside the control rooms. Ensuring 24/7 capabilities on a day-to-day operation, their staff uses the system to manage any individual incident that requires documentation and follow up, and also provides them with the capability to send notifications to other team members around the state.</p> <p>Details: DLAN provides the support the Power Authority needs to manage their critical business. For example, the DLAN system was able to immediately send Incident notifications to their predefined list of members that needed to be notified of a specific situation. In a matter of seconds – an operator (via PC or mobile device) could automatically generate a notification to particular staff across the state. The ability to provide information at a moment's notice is essential to their operation. As a web-based tool, DLAN allows offsite staff to quickly log in and provide status and information to the location at headquarters.</p> <p>A seamless transition has been provided to the Power Authority as this organization has transitioned from a deprecated, silo-ed system to DLAN. This allows the control rooms onsite and offsite staff to efficiently and easily participate at any time, and eliminates duplication of efforts as they manage their daily or emergency affairs. As situational awareness tool, NYPA utilizes DLAN to manage daily events and keep track of a variety of information that affects their state-wide operation. Utilizing the GIS mapping tools and Status Boards, information can quickly and efficiently be shared.</p> <p>This client also employs a totally separate Training Site. This allows users to have training any time on a DLAN system set up exactly like the live site. In addition the training site can be used for exercise play without the need to worry about interfering with daily operations.</p>		

Reference #5 LAMACS System - City of El Segundo California

LAMACS-City of El Segundo, California, Emergency Management/Disaster Preparedness			
Contact Person:	Randal Collins, Emergency Management Coordinator		
Contact's Email:	rcollins@ahimta.org		
Address:	LAMACS - City of El Segundo California 350 Main St., El Segundo, CA 90245		
Contact's Phone:	(310) 524-2366	Date of Service:	2021 - Present
Modules:	DLAN Advanced with: Asset Tracking, Mobile Responder, Emergency Management Pack, Chat, GIS Premium, Phonebook Premium, Status Board Builder, Streaming		

	Video, Ticket Manager Premium, Reference Library, Resource Database, Status Board, Reference Library, Training site.
Project Description	<p>Summary: Buffalo Computer Graphics was recently selected to provide DisasterLAN incident management software to the 88 cities within the Los Angeles Operational Area. In late 2020, the cities within the LA Operational Area worked together to procure emergency management software for the region. The project was spearheaded by Randal Collins, the City of El Segundo Emergency Management Coordinator. He, along with fellow colleagues, saw the need for a coordinated, integrated common operation picture that spanned the entire County and connected all the emergency managers and other stakeholders onto one platform.</p> <p>BCG provided a DLAN Advanced system that would provide elected officials, city managers, department directors, operational managers, and other partners with situational awareness of incidents and events. The system allows all of the municipalities to manage situations within their jurisdictions and also to coordinate with each other on multi-jurisdictional emergencies. They also chose to utilize BCG’s Platinum level of maintenance to afford them the highest level of support coverage. BCG provides a hosted solution for 500-1000 users, and the system continues to expand as they add additional areas and organizations. Because of their rapid and ongoing expansion to additional organizations, training has been a huge part of the installation.</p> <p>Details: After a competitive RFP process, BCG’s DLAN software was selected. One of the main reasons DLAN was chosen is that the system does not include individual user licenses. This means that various partners across municipalities could be added to one system quickly and easily. The intuitive user interface meant new users need minimal training to effectively use the system. This makes it easy to bring in additional parties during a crisis. This customer chose to add a premium level of GIS to enhance their system mapping capabilities, along with Ticket Manager Premium and the Incident Action Plan Module.</p> <p>The Los Angeles Operational Area liked DLAN’s flexible and modular design that allowed them to add on features as needed. DLAN’s system is also fully configurable, so the system was setup to fully meet the exact needs of this critical area in California. Collins notes “You don’t get that level of customization with other products.” He also remarked that the in-depth implementation process really helped the cities work through the various processes and workflows necessary to make a cross jurisdictional system work for all involved. Collins commended the BCG team on their responsiveness throughout the process and even noted that the team proactively pushed the project forward.</p> <p>“BCG really took the reins and guided us through the entire process. They were relentless in scheduling meetings and making sure forward progress kept happening... BCG’s commitment to project management really took the burden off of the emergency management staff and saved them a lot of time.” Randal Collins – City of El Segundo</p> <p>The City of El Segundo is utilizing the system for their own daily and emergency operations and for creating Incident Action Plans as needs arise. Additional municipalities are still being added to the system. Currently the plan is for DLAN to be used as the incident management system for Super Bowl 2022, which will be played at</p>

	SoFi Stadium in Inglewood, California. As other municipalities are onboarded the vision of real-time multi-jurisdictional situational awareness and collaboration will be fulfilled.
Project Start & Finish Dates	2021 - Ongoing 4 year contract

3.2 Vendor shall provide references for unique projects that started and/or were completed, and/or are in execution in the past Three (3) years.

Please see the answers provided in 3.1 above.

3.3 Vendor shall provide at least One (1) of the references above in 4.3.1.1 from United States public sector/government clients.

NYS Division of Military and Naval Affairs (NY DMNA)

NYS Division of Military and Naval Affairs			
Contact Person:	Staff Sergeant Robert Spohr		
Contact's Email:	robert.t.spohr.mil@mail.mil		
Address:	NYS Division of Military and Naval Affairs (DMNA) 330 Old Niskayuna Road Latham, NY 12110 United States		
Contact's Phone:	518-786-6104	Date of Service:	2009-Present
Modules:	DLAN Enterprise with: GIS Premium, Mobile Responder, Watch Command, Chat Client, Communication Center, Briefing Notes, ICS Forms, Incident Folders, Phone Book, Reference Library, Ticket Manager, Calendar		
Scope of Work:	<p>Summary: BCG installed a multi-functional DLAN system for this military operation to manage Army National/NY, State Naval Militia, Army Air Guard – Air Wing Military Operations, and Guard-Air Wing Military Operations. To address their numerous responsibilities and requirements they have many of DLAN's optional Modules including: Watch Command, GIS, Reference Library, and Briefing Notes. The system was originally installed as customer hosted and in 2017, they opted to host it in the cloud. Recently the system has been utilized for the air operations activities for the Lake Ontario Flooding situation as well as recent COVID-19 responses.</p> <p>Details: Buffalo Computer Graphics, Inc. (BCG) was the prime contractor and managed the initial installation, training, and all enhancements and re-configurations since 2009. DLAN software is used in the Joint Forces Headquarters (JFHQ) for military and naval affairs in New York State. DLAN plays a critical role in the 24/7 Joint Operations Centre managing day-to-day requests and monitoring potential hazards for the New York State Army and Air Force National Guard as well as naval and maritime forces in New York. The system is utilized to manage numerous tasks and requests for assets. During COVID, DLAN's work flow flexibility was utilized by also managing end-to-end requests coming from the Javits Center field hospital in New York City.</p> <p>The system was successfully utilized to manage assets and activities for air operations missions in the critical Hurricanes of Sandy, Irene, and Lee. The JFHQ is located in Colonie, New York a short drive from the capital of Albany where DMNA works very closely with the Department of Homeland Security and Emergency Services for the State of New York who also utilize DLAN for all incident management and preplanning activities in the State. The DLAN solution utilized by DMNA is a feature rich version of the software designed to provide comprehensive end to end Air operations management of inventory, equipment tracking functions. The Watch Command module</p>		

	functions as a 24/7 Joint Operation Centre watch point to log and manage potential or ongoing activities. It also serves as a dashboard to monitor a variety of incoming communications, which can be posted to actionable work order tickets. These singularly logged items in the Watch Command can be bundled together into a larger collective if the situation escalates. Alert information is also monitored from this module, including IPAWS messages.
--	--

3.4 Vendor shall provide a minimum of three (3) relevant references to demonstrate that it has proven experience in managing hosted/on-premises EMIS solutions at a statewide level. All referenced Solutions shall be currently operational in a production environment. This information shall be provided prior to contract award. The document provided as a reference shall include the state, organization name, point of contact, start and end date of implementation.

Please see the answers provided in 3.1 & 3.3 above.

Reference #1 Oregon Department of Human Services

Oregon Department of Human Services (ODHS) – Emergency Management	
State:	Oregon
Organization Name:	Oregon Department of Human Services (ODHS) –Emergency Management
Point of Contact:	Steve Pegram, Executive Director
Start and End Date of Implementation:	8/17/21-Present
EMIS Modules Implemented:	This is a DLAN Premium system with the following modules: Bed Tracking, Finance, GIS Premium, HICS Forms & Job Action Sheets, Special Needs Module, Chat, Communication Center, GIS, Incident Folders, Mobile Responder, Phonebook, Phonebook Premium, Reference Library, Resource Database, Social Media Basic, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Healthcare Industry Pack, ICS or IMS Forms Module, Incident Action Plan Module, Role Checklist Module, Situation Report Module, Damage Assessment Form, Report, & Board, Road Closure Form, Report, & Board, Role/Task Status Report & Board, Shelter Management Form, Report, & Board, and the Sheltering Module

Reference #2 NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)

New York State Department of Homeland Security and Emergency Services	
State:	New York
Organization Name:	NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)
Point of Contact:	David Smith, Operations Section Chief
Start and End Date of Implementation:	2004 - Present
EMIS Modules Implemented:	This is a DLAN Premium system. Modules include: Chat, Communication Center, GIS Basic, Incident Folders, Mobile Responder, Phone Book, Phonebook Premium,

	Reference Library, Resource Database, Social Media, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Emergency Management Industry Pack, ICS, IAP, Role Check list, Situation Reports, Damage Assessment, Weather, Separate Training Site, Watch Command
--	--

Reference #3 NYS Division of Military and Naval Affairs (NY DMNA)

NYS Division of Military and Naval Affairs	
State:	New York
Organization Name:	NYS Division of Military and Naval Affairs (DMNA)
Point of Contact:	Staff Sergeant Robert Spohr
Start and End Date of Implementation:	2009-Present
EMIS Modules Implemented:	DLAN Enterprise with: GIS Premium, Mobile Responder, Watch Command, Chat Client, Communication Center, Briefing Notes, ICS Forms, Incident Folders, Phone Book, Reference Library, Ticket Manager, Calendar

4. GENERAL REQUIREMENTS

4.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below. Contract Items must meet or exceed the mandatory requirements as shown below.

BCG asserts that it shall provide West Virginia Department of Emergency Management with a software solution and services that meet all mandatory requirements below.

4.2

4.2.1 Emergency Management Information System (EMIS)

BCG is the creator and sole provider of a commercially available Emergency Mangement Information System (EMIS) with the brand name of DisasterLAN™ or DLAN for short. The system is modern, effective, completely customer configurable, and has been in use by agencies, counties, and states across the USA and Canada since 2003. BCG provides regular updates to the software every ten weeks and provides all help desk, customer support, and services work in-house with our staff in the USA.

4.2.1.1 Vendor must provide an EMIS solution that features the following:

4.2.1.1.1 Incident Reports

- 1. The EMIS shall enable authorized users to create, update, and view incidents from browsers, and mobile applications.*

Incidents

DLAN can be used to track and manage incidents, trainings, exercises, events, and daily activities of any size or scope from browsers or mobile apps. Whether used to manage a pre-planned event, severe weather, a crisis

situation, routine incidents, or a disaster, DLAN provides tools for incident tracking on many levels. With task, mission, and resource management tools, emergency communication tools, and custom status boards, DLAN makes it easy to track, manage, and report on multiple incidents and events from one unified mobile ready solution. Incident security features allow administrators to easily lock down an event or incident to just the people that need access to it. When using DLAN to respond to multiple incidents at once, the confidentiality of data between incidents can be enforced using the incident locking system. This allows the user to be granted access to information within specific ongoing incidents in the system, while restricting access to others. Information can be shared between incidents, which allows selective sharing of information. Incident security features allow administrators to easily lock down an event or incident to just the people that need access to it. Filters within the system make it easy to look at data specific to the incident the user logged into, as well as giving them the ability to look at data across multiple incidents simultaneously. Filters within the system make it easy to look at data specific to the incident the user logged into, as well as giving them the ability to look at data across multiple incidents simultaneously. Individual events are logged in the system as tickets within a designated incident. These tickets contain a variety of information as the customer chooses and can also be color-coded for status and priority in the system so administrators and users can quickly see the status. Issues can be quickly logged in an incident as a ticket with simple guided entry data entry tools. Task for ticket completion can be automatically assigned and routed to a responsible individual or Role through automated custom work flows in DLAN. DLAN provides simple color-coded ticket statuses and priorities for tracking and rapid status overviews.

Incident Creation

Incident Configuration allows an administrator to easily create, set security settings, and archive emergency incidents and planned events from a desktop or mobile device. Incidents can be created using either a traditional form or wizard interface. Active incidents are available for designated users to log in to and all data entered is tagged with the incident for management during and after the incident. This helps with creating after action reporting (AAR). In DLAN an Incident is defined by following government standard ICS and NIMS guidelines.

DLAN can run multiple simultaneous incidents and supports all levels of incidents from local, county, regional, state/provincial, and federal levels. The Lock-Down Incident Security feature allows separate incidents to be created for different groups, agencies, or municipalities with access restricted to only their users. Administrators can also set the default incident for users to log in to and can view and access archived incidents and events.

Administrators can send out automated notification messages to selected distribution groups when a new incident is created or when an incident is edited. They can also set the default incident for users to log in to and can view and access archived incidents and events. Another major feature of DLAN's Incident Configuration function is the ability to run a spot report or create an after-action style hot-wash report. Incident reports are comprehensive chronological reports detailing all additions and modifications to records and data that occurred during an incident or event. Reports can be filtered down to a specific date range or type of records, including tickets, messages, broadcasts, Status Board items, uploaded Incident Folder Documents, Situation Reports, ICS Forms, Incident Action Plans, and GIS Map Snapshots. Like other DLAN reports, the Incident Report can be exported or printed as needed.

When an incident is over it can be Archived by the administrator. At that point when an incident closed it is considered complete and no more information can be logged for the event. The information can still be accessed by select individuals with the GO-TO function. The Archived incident can be utilized for a variety of after action reviews including: recovery activities, reporting, or financial reimbursements.

Task & Mission Management

Task Management is achieved in the DLAN system with the Ticket Manager module. Each task or mission in the system is represented by a ticket. Tickets can include other associated elements such as forms, maps, checklists/guides, attachments, and other data. The module also has a full suite of progress tracking capabilities

including the ability to select a ‘type’ and ‘kind’ to help categorize the ticket and the ability to set statuses and priorities. Tickets can be tasked to a role that is responsible for updating or contributing to the ticket. Tasking is achieved by routing the ticket to one or more roles – this will make the ticket appear on the dashboard homepage for users in that role.

Built in to DLAN is the ability to log issues as individual ‘tickets’ with guided data entry tools. Tickets can be assigned as tasks to roles manually or with automated custom workflows and their progress can be tracked with customizable color-coded statuses & priorities within the Ticket Manager module.

Mobile Application

The Emergency Management industry is rapidly shifting towards mobile centric operations; with support for almost all devices, DLAN ensures you won’t be left behind. With DLAN, mobility is not an afterthought. BCG engineers approach development with a “mobile first” perspective where modules and pages are built to operate on tablets and phones early on in the development process. From there, DLAN engineers build our modules so that they are responsive; automatically scaling their capabilities, views, and features based upon the screen size of the end user’s computer or mobile device.

These “mobile first” methodologies also follow through with our reporting and exportability of data, allowing users to make use of information in the field even when the user cannot be on DLAN. All DLAN data, including reports, maps, emails, and images, can be exported using common exporting formats such as PDF, Word, Excel, and CSV, which can be read by most wireless handheld devices and laptops. These reports can be instantly sent to mobile users via email, Twitter, or other multimedia pathway.

In general, DLAN is accessible on any mobile browser that fully supports JavaScript, session-based cookies, HTML 5 technologies, and other modern web browser features. Some mobile devices that support DLAN natively (i.e. no app required) include, Apple iOS devices, Windows Mobile devices, and Android devices.

All areas of DLAN work within a mobile environment when connected to a Wi-Fi or cellular network. DLAN also includes a specific Mobile Responder App that can be used when unable to connect to a network. The app is designed for iOS, Android, and Windows and is available from the Apple App store and Google Play store.

The app stores all report data locally on the device and automatically sends it to DLAN whenever a Wi-Fi or cellular internet connection becomes available. This "store and forward" capability ensures data integrity and usability under the most adverse conditions. The app includes the ability to use either standard or custom forms. Filling out a mobile form using the app is a quick process completed by filling out fields, attaching photos or videos, and clicking the Submit button.

2. The EMIS shall geolocate the incident based on the incident location data and update the Common Operating Picture (COP).

The DLAN EMIS automatically geolocates all addresses entered into the system for incidents and other records. Additionally, entering an incident, also allows users to draw a point, line, or polygon (shape) on the map if an address location is not available. Geolocation tools in the system support multiple geocoders from different sources such as ESRI or local geocoders created by WVDEM’s GIS department. Because incidents (as well as all other records such as contacts, facilities, assets, and more) are geocoded, they all appear on the GIS Common

Operational Picture Map automatically without any additional steps needed to make them available. Users can toggle incidents, tasks, resource locations, and other data on or off to customize the map as needed.

In addition to incident location data, the COP can also be incorporated into a DLAN EMIS Status Board (dashboard). Status Boards consist of configurable panels that display information from various sources. Panels can be made up of situational awareness information, including messages, PDFs, images, social media feeds, Mission reports, and task reports. Additionally, Status Boards can incorporate saved GIS maps with preset data layers, basemaps and extents, animated weather radar imagery, links, websites including other DLAN pages, and more. All content is live and continuously updates for real time on the COP for situational awareness.

3. *The EMIS shall receive, record, and log incident situation reports submitted by authorized users. These reports may contain but not limited to the following personal identifiable information (PII):*

- 4.2.1.1.1.3.1 *First Name*

- 4.2.1.1.1.3.2 *Last Name*

- 4.2.1.1.1.3.3 *Phone Number*

- 4.2.1.1.1.3.4 *Address*

The EMIS solution will not store medical records or other data related to a person's health conditions.

DLAN's Ticket Manager Module includes a unique ticket forms feature for logging incident situation information and is able to receive, record, and log incident situation reports submitted by authorized users. These reports may contain but not limited to the following personal identifiable information, including: first name, last name, phone number, and address.

Ticket Forms can be created, uploaded, and edited by system administrators and help to standardize user data entry. These fully customizable forms allow administrators to decide exactly what information they want collected for particular types of incidents, requests, offers, tasks, reports, etc. Ticket Forms can contain any combination of fields, labels, grids, drop-down lists, and check-boxes that are needed in order to create a working electronic form that fits the needs of the organization. Ticket Forms can be associated with different ticket types and kinds, allowing for forms to be automatically attached as part of a required workflow when needed. Additionally, forms created by the user can be used with the DLAN Mobile Responder App. Offsite users can fill out and submit forms from the app (e.g.: damage assessment form) and it will sync back to the DLAN system automatically and be converted into an actionable ticket with the filled-out form attached.

The system allows users to report incidents using an online form. System forms are all secure, and can be submitted through the website or can be submitted from the Mobile App. Customer administrators can create their own incident report forms or edit the default ones that come with the system.

In addition to reporting incidents using a secure online form, users (or non-user stakeholders) can report an incident by email. Email messages sent to the system are automatically received and converted into a report ticket for reply or follow-up action.

4. *The EMIS shall provide a component to create, collect, and notify data related to different type of incidents that are reported through the Watch Center. These are the reports include but not limited to: Arson Investigations, Tip Rewards, Mine Incidents, Workplace Safety Tips, Safe Schools, Industrial Incidents, State Interoperable Radio Network (SIRN) operators' reports, and Infrastructure Protection*

Incident Notification (IPIN). The system shall allow the user to attach videos, photos, documents, and call recordings.

DLAN's Watch Command module includes 24/7/365 monitoring and communication tools to support Duty Officers & steady state operations. It provides the ability to receive up-to-date news and incident reports from staff and agency representatives across the state. Information is also aggregated from several external sources including incident reports into one internal location to facilitate the review and processing of information.

Ticket Forms, used in the Watch Command module will allow WVDEM to create data collection fields for use with incident reports. This means that users can select the incident report kind from a drop-down list (arson, tips, etc.) and then have relevant fields appear to guide the collection of further information. The form can be filled out from either the website or from the mobile app. The mobile app supports offline use and both the website and the app allow the user to attach photos, videos, documents, recordings, and other files. Forms can be created and configured as needed by WVDEM administrators or BCG support staff.

5. The EMIS shall enable the system users to change the status report and the system sends the report automatically as an email notification.

The system tracks incident reports as well as other information reports, donations, and requests, in a Ticket. The ticket interface includes key fields for managing information such as a priority field, status field, routing (assignment) field, and more. A user with can adjust the status of a report ticket by simply editing the ticket and clicking on the Status Field. This will open a drop-down menu from which the user can adjust the status. As soon as the user saves her or his changes, the status of the report will update everywhere in the system. Changes to report tickets, including status updates will trigger both internal notification s to users logged into the system, as well as email and text message notifications to users who are not logged into the system.

WVDEM administrators can control the list of available statuses, which users can change report statuses, and the rules regarding how automatic email notifications work.

6. The EMIS shall select from a dataset the right contacts who receive the email notification.

DLAN supports user alerts via multiple methods including both in-app alerting, external email and SMS notifications. Alerts can be triggered manually, or automatically based on system configuration settings. Email notification settings can be configured by WVDEM administrators on a user account basis, on a role/position basis, or on a system-wide basis. This solution offers a effective combination of ease of use and granular flexibility as needed. Examples of email notification capabilities are listed below.

Note: For privacy law reasons, users can opt-out of automatically triggered alerts to their email or text message device. However, in-app alerting to users who are logged into the system will always notify users.

Incident Event Alerts:

When a new incident or event is created in the system, the initiator can choose to trigger a notification as part of the incident/event creation process. The notification can be sent to users within the DLAN app (in-app) via DisasterLAN Mail (DMail) message which will appear in the user's mailbox, or it can be sent out to external contacts using email, SMS via SMTP (text message), distribution group, scenario contacts list, system to system

integration, IPAWS, or other communication channel. Incident and Event Alerts can also be configured to trigger automatically to any of the methods listed above based on system settings/rules.

Resource Request Ticket Alerts:

Automated email and text message notifications can be sent to users when a Resource Request has been tasked to their role but there is nobody logged in to handle it. Users who have access to that role will receive an email or text message notification (according to their preference) alerting them to this and providing a URL link to login and view the information.

Mission / Task Ticket Alerts:

Automated email and text message notifications can be sent to users when a Task or Mission Ticket has been routed to their role but there is nobody logged in to handle it. Users who have access to that role will receive an email or text message notification (according to their preference) alerting them to this and providing a URL link to login and view the information.

Other Requests/Polling of Stakeholders:

Agency Report Notifications: Automated email and text message notifications are also available for situation reporting. If a role has been tasked to complete an agency report for their role or organization and they have not completed it by the time the end of the operational period approaches, then users in that role will receive an automated notification asking them to login and complete their agency report.

DLAN also provides a number of methods for both automated and manually triggered notifications.

Accept Remove System: When a manager or authorized user assigns a task ticket to one or more roles, the receiving roles can use the accept/remove feature to either accept responsibility for completing the task, or remove themselves from the routing list which will decline the task and remove it from their role-specific view. Of course, an administrator or authorized user can re-route the task to a role after they have removed themselves. This feature is often used to poll several roles or agencies to see who can supply a resource or has the current capacity to complete a task.

CC Alert Feature and Email Reply

Notification Profiles: Users or administrators can create contact records for people in the DLAN phonebook. Part of the contact record allows a user to choose notification methods such as cell phone, email, SMS (text message), pager, etc. These contact methods are used when sending a manually triggered notification message.

Notification Distribution Groups: DLAN allows an administrator to create distribution groups which can be used to send outgoing messages. These distribution groups can be used to send an email, ticket, incident action plan, or ICS form.

Notification Scenarios: Scenarios work similarly to notification distribution groups, however, they allow an administrator to tie a distribution group to an emergency scenario. The concept is to allow preplanning personnel to create a list of people to contact in case a specific emergency occurs. Then a message can be

blasted out to contact all the right people immediately. Common scenarios are Severe Weather, Hurricanes, Tornadoes, Hazmat, Flooding, Train Derailment, Mutual Aid, etc. As long as WVEMD knows who they need to contact in a specific scenario, they can create a notification contact list ahead of time and this will allow them to gear up the EOC with the right folks during an emergency without having to spend the time to organize a contact list of necessary participants and call everyone.

7. The EMIS shall offer a mobile application and system interface to update the contacts notification dataset.

The EMIS includes native mobile applications for Apple iOS devices (e.g. iPhone, iPad), Android devices, and Windows devices in addition to the mobile-friendly web-based user interface. Users can login to the system from a mobile device and update the contacts notification dataset as needed. These changes are reflected in real time in the system as well as for users who are logged in through the mobile app.

The system also automatically updates contact information in several cases. First, when a user logs into the system they are asked to confirm their contact information. Updates at the login screen are automatically propagated to the user account, user list, and other areas of the system. Second, changes to contact information in the system's Phonebook Module automatically propagate down to the mobile app's online/offline contact directory as well as to the system's address book which is available when selecting a contact for a message, email, or ticket/task assignment.

8. Depending on the type of incident, the EMIS shall pull data to auto-populate reports.

DLAN can pull data to auto-populate various reports. The reports are designed to support both emergency situations and day to day operations. Modules such as Ticket Manager can easily be structured to create detailed reports on tasks, requests, donations, reports of information, Action Plans, Situation Reports, and more. All reports reflect real-time updates. As soon as a user makes a change, all reports are updated automatically and relevant data is auto-populated. Additionally, all reports are searchable and sortable, and can be exported off the system using the export tool.

Many of the modules in DLAN allow users to create custom reports as well. BCG's easy to use tools allow administrators to lay out new documents, boards, forms, links, and other pages as needed, giving DLAN users a powerful way of managing the various reporting and input needs of each incident.

Landing pages or dashboards allow administrators to control what a user or role is directed to once logged into the system. Additionally, administrators and users can customize the content they see on these boards in an unlimited fashion. Boards can include additional custom reports that contain either standard or customized data. An example of this would be a map report on a board. Map reports can include auto-populated information, standard DLAN data (events, incidents, requests, reports, etc.), and can include agency, role or user specific data such as critical facilities, shelters, schools, etc.

9. The EMIS shall offer a mobile application and system interface to update those datasets required to auto-populate a report.

The DLAN Mobile Responder App provides a system interface for users to update datasets to auto-populate a report. The app allows users to fill out and submit forms from the mobile app that are then synced to the DLAN web application and are automatically turned into actionable tickets with all data from the report auto-

populated into the ticket report. This provides field staff with a way to submit resources requests, reports of information, damage assessments, and other types of data from the field using a native iOS, Android, or Windows app.

10. The EMIS shall offer a system interface to update select lists, such as the agencies list and resources list. The system shall control names' duplication.

The DLAN EMIS provides an administration interface to authorized users. The administration interface allows admins to update drop-downs, select lists, and other data fields and configuration settings as needed. All changes occur in real time and are available to users as soon as the administrator completes them. For example, a list of organizations, agencies, or roles on the system can be updated by an administrator and those changes will appear for users immediately. The administration interface typically checks for duplicate names or entries upon creation. Some modules, such as the Phonebook also have administrator reports that can be run to check for similar personnel or agency records using a fuzzy logic to provide a list of potential duplicate entries. The administrator can then choose which record to keep and which to remove.

11. The EMIS shall offer the option to send those reports as part of an email's content (email body).

The system provides the ability for users to send reports off the system as an email. Email reports can include the information as an attachment file, or as content within the body of the email, or both. Users simply click the checkbox next when sending a report to select which way it operates.

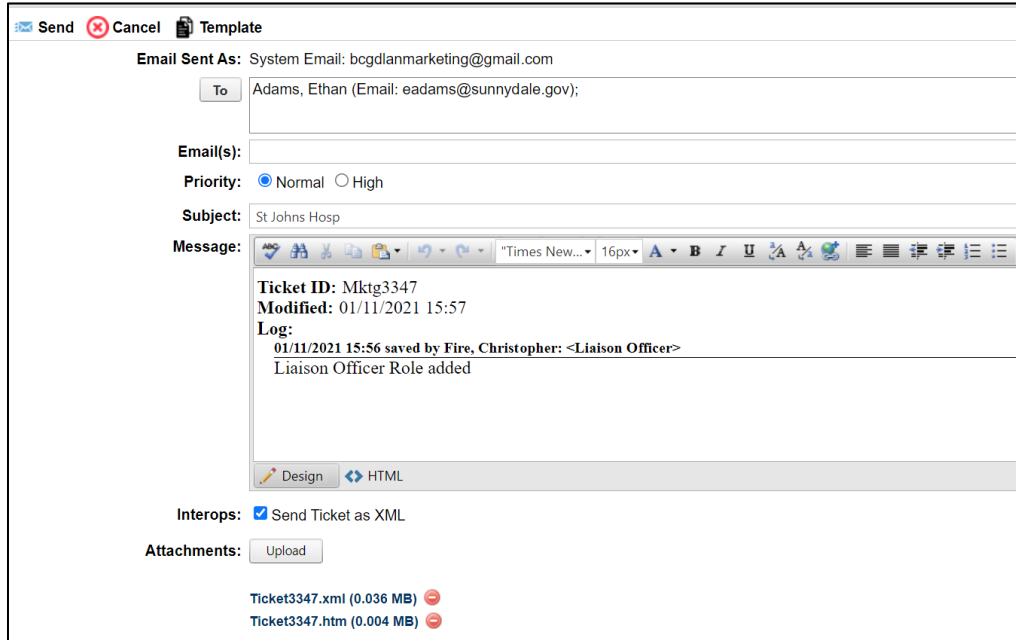


Figure 1: Email Reports

12. The EMIS shall offer the option to call the phone numbers included in an incident report. It shall be possible from a mobile application and a system desktop/laptop/tablet interface. It is understood that the mobile device (phone or tablet) has a data plan.

The DLAN system's mobile app allows users to call phone numbers that appear on the contacts tab of incident report tickets. For web-based users, if your device browser has the capability to detect phone numbers, you are able to call those numbers included on incident reports in DLAN.

13. The EMIS shall offer the option to print incident reports. The printed reports shall include images, and the attachments' list.

All incident report tickets can be printed along with images and attachments. Print options include the following:

- Print Table – this will print a tabular view of all incident tickets in the user's current report or view
- Print Ticket – this will print an individual incident report including any attachments such as images or associated files.
- Print Packet – this will print an individual incident report including all supporting evidence (images, files, forms, etc.) in a format that is suitable for use for reimbursement evidence.

Additionally, any incident report can be exported in PDF format and many can also be exported to Word, Excel, and CSV.

14. The EMIS shall geocode and present as a layer incidents per type of incident, and to include those layers in the COP. Those layers must be updated based on a data/time. It is understood the system is not replacing the whole dataset. It is updating based on new reports.

The DLAN system can geocode and present as a layer, incidents by incident type, and to include those layers in the COP viewer. The layers will be updated based on a data/time, and is understood the system is not replacing the whole dataset. DLAN updates based on new reports of information. DLAN's GIS module provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

DLAN's GIS functionality also allows you to fuse together geospatial information from virtually any external or internal source onto one common display. DLAN ensures that you are always viewing the latest information. User-friendly tools also allow users to interact with underlying data. For example, tools for identifying data and creating buffers based upon point features, polygons, or ALOHA plume models allow users to drill down and see information that is pertinent to the incident at hand. Data can then be used to make decisions, and if desired, exported for use in other applications.

From an administrator's standpoint, DLAN's configuration tools make managing and adding new data sources or basemaps quick and easy without needing any GIS expertise. Data can be organized into categories that appear on a touch screen friendly ribbon, making locating and toggling information on and off a snap, and data layers can be locked down to select users.



Figure 2: GIS Map Updates

Integrated Solution

In addition to incorporating key external data, DLAN GIS also displays data from other DLAN modules automatically. For example, incident report data entered in to a ticket appears on the map as a layer automatically. Incident report layers are created automatically based on Ticket Manager Module report criteria such as incident type, category, date/time, and other filterable criteria.

Additionally, users can add and edit incident report tickets directly from the map interface.

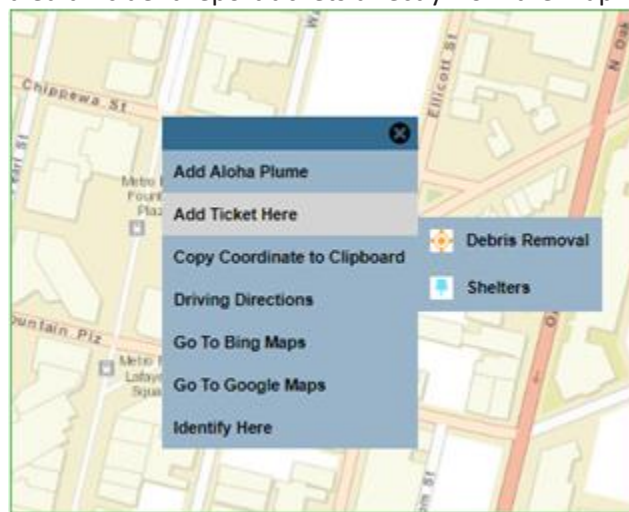


Figure 3: GIS Map Requests and Reports

15. The EMIS shall offer a dashboard per report type to monitor the notification status, access contact information per report type, and link to the datasets that are required to auto populate a specific type of report.

The DLAN EMIS Ticket Manager Module allows users and administrators to create custom reports of information based on filterable criteria including report type (incident report ticket kind). When the ticket manager report is created the user can select the columns of data that will be displayed in the report including notification status icons, contact information, links, form data, field data, dates/times, and other information. Once created, the

data returned by each of these reports populates automatically and is be viewable in a tabular format, or in a Status Board (dashboard) format.

See section 4.2.1.1.2 for more information regarding the Status Board Module dashboard capabilities.

16. The EMIS shall offer the option to export data as a .csv or .xls format.

DLAN includes an export feature that is available on all data tables, lists, and reports. With one click users can export data out of DLAN to MS Word, Excel (.xls), CSV, or PDF formats for further analysis. Data can also be emailed to outside stakeholders by clicking the Forward button. This attaches the document, file, or ticket to an email and sends it off the system to the selected or entered recipients.

4.2.1.1.2 Incident notification. The EMIS shall support automatic notification and support organizational as well as external email addresses.

DLAN supports automatic user alerts via multiple methods including both in-app alerting, external email and SMS (text message) notifications. Alerts can be triggered manually by a user sending a message or forwarding content to an email address. Additionally, notifications can be sent automatically based on system configuration settings. This includes the ability to automatically send out incident information to users who are offline, or based on business rules.

1. The EMIS must enable authorized users to assign or remove members of the contact lists to associated message groups to facilitate rapid dissemination of messages to specific sets of recipients.

DLAN allows authorized users to assign or remove members of contact lists to associated message groups facilitating rapid dissemination of messages to specific sets of recipients. Distribution Groups are an easy way to incorporate a set of contacts into one easy selection when sending out a message from the DLAN Communication Center. Distribution Groups can consist of DLAN Users, Phonebook Contacts, Custom Recipients, COG's (Collaborative Operating Group's), or any mix of them all. Distribution groups can be used to send an email, ticket, incident action plan, or ICS form.

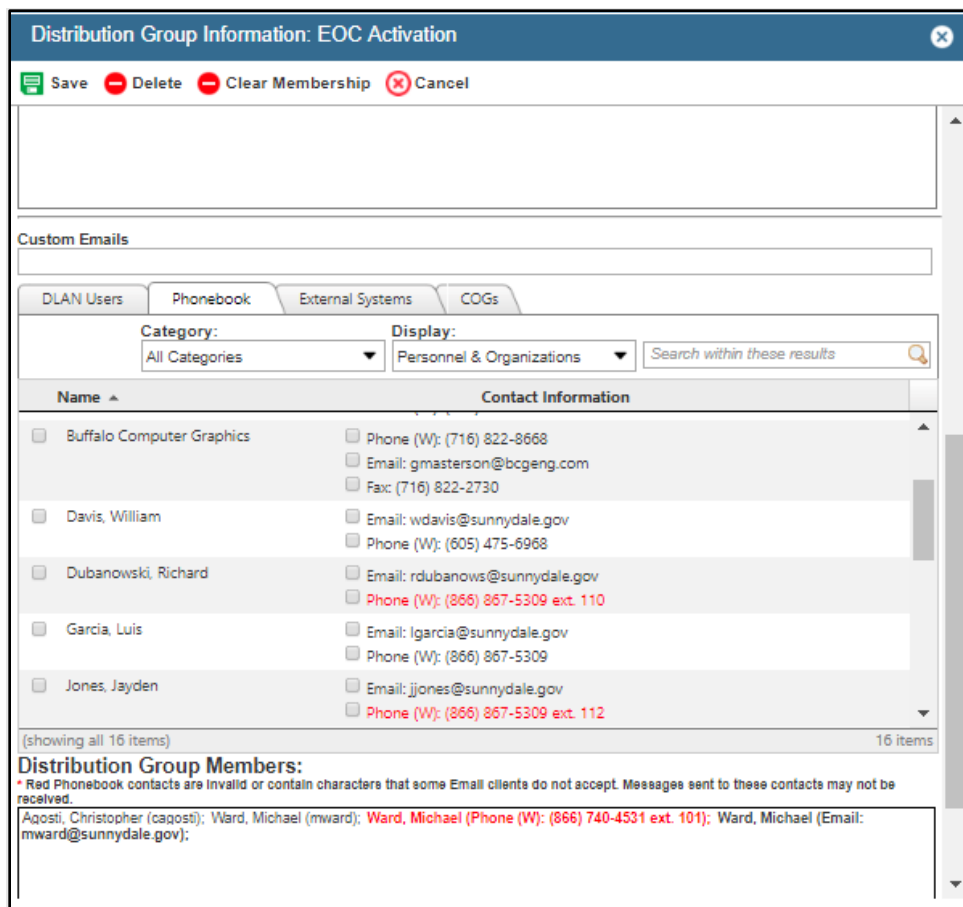


Figure 4: Distribution Group

4.2.1.1.3 *Contact lists and Directory. The EMIS shall enable users to create contact lists for emergency management staff and external contacts.*

DLAN’s Phonebook allows users to quickly create contact lists for emergency management staff and external contacts.

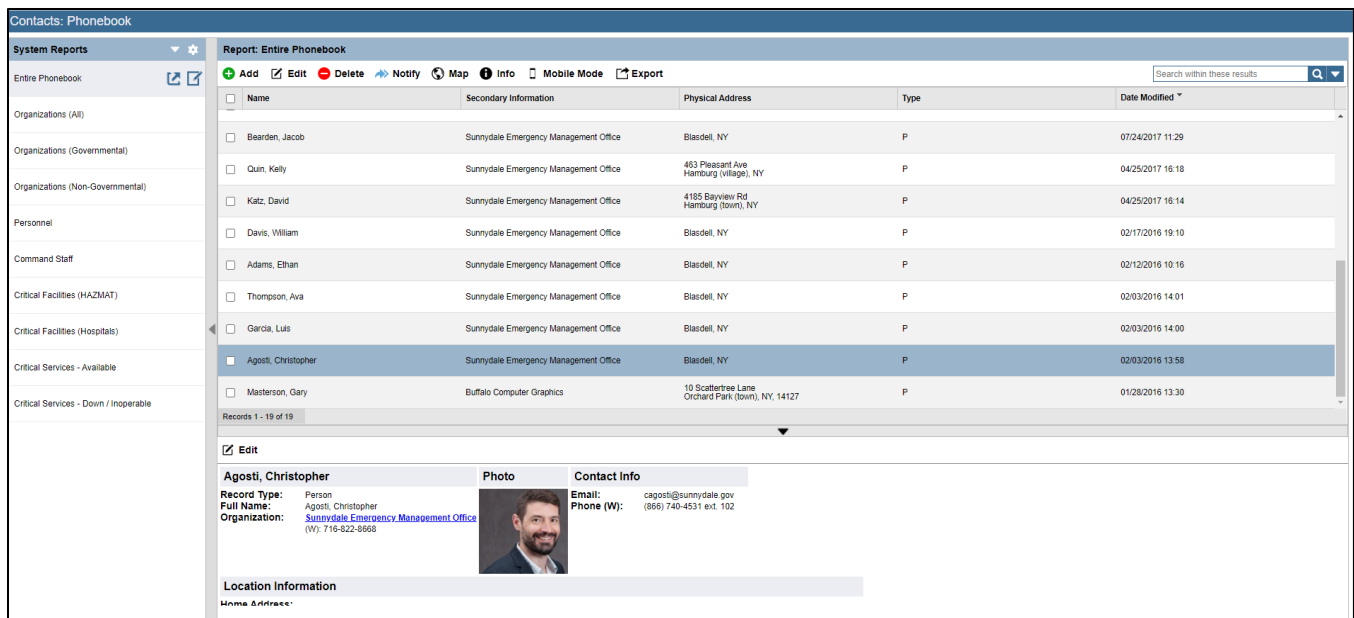


Figure 5: Phonebook Report

DLAN’s Phonebook report engine allows users to easily create reports on personnel and critical facilities that are important to them. Tools allow reports to be created based on filters such as trainings, skill sets, categories of personnel, categories of facility, and locations. Once created, these reports immediately become available for use in other modules, such as GIS Premium or Status Board Builder. They can be used as layers on maps, bookmarked locations in map reports, and panels in status boards or landing pages. With this feature you can easily build real time views of staff that have specific qualifications, facilities that provide particular types of services, vendors that provide a required resource, and other types of critical facility reports that would be beneficial during an incident.

These lists can also be turned into distribution groups for easy messaging, see 4.2.1.11. for additional details.

1. *The EMIS shall use these contact lists to send reports, email, and notifications.*

The Notify button in the DLAN Phonebook allows users to notify some or all individuals listed in a Phonebook Report. For example, a phonebook report can be created to show all users on the system from a specific jurisdiction, or with a specific skill or training (e.g. firefighter, ops section chief, etc.). Then the user only must run the report to return the relevant records, click the checkbox to select them, and click Notify to send an email, report, text message, or notification to those individuals.

2. *The EMIS shall eliminate the duplication of effort by enabling users to update contact data one time and update the instances where that contact is used.*

Updating any contacts in DLAN’s Phonebook automatically updates distribution groups and communication center recipients. This eliminates any duplicate of effort, and keeps contact data aligned and current for all users.

4.2.1.1.4 User-based permissions. This system shall be capable of assigning user-based permissions to data. These permissions will be based on security levels determined by system administrator(s). The system will be capable of determining access to data based on user permission level.

Security

DLAN includes a robust and flexible security utility that is part of the system administration module. It provides for multiple layers of security and access control throughout every level of the system. The permissions structure in DLAN is tiered and can be configured by the customer to have granular security permission, broad security permissions, or any range in between. DLAN accomplishes this flexible and intuitive security structure by implementing administrator defined security groups which are separate from user accounts and roles. These security groups are composed of several individual security permissions.

The principle of least privilege is the guiding methodology for security in DLAN. Users are only provided the minimum level of access necessary to perform their job functions in the areas of the system that they are required to use. Other areas of DLAN remain invisible or inaccessible. In addition to securing information, this also simplifies the number of options on the end-user's user interface, which makes just-in-time training quick and easy. It also encourages an ICS based workflow process for handling information flow in the EOC as each end-user has a clearly defined job duty and passes information along to the next person in the chain.

Administrators may configure an unlimited number of user accounts, groups, and roles. Groups and roles may be assigned to a user account through the use of a simple checkbox system. Users may have multiple groups and roles if they are trained for multiple positions, this allows them to retain one account and toggle between views as needed. DLAN comes with several default security groups already created, and during the configuration period BCG trainers will work with you to create other security groups and user accounts as needed. Administrators can change user's security permission on the fly and it will apply instantly without the need for the user to log out. This flexible and intuitive security system will cover all of your needs and allow system administrators to change or add privilege levels on the fly during an incident.

Export Button

DLAN includes an export feature that is available on all data tables, lists, and reports. With one click users can export data out of DLAN to MS Word, Excel, CSV, or PDF formats for further analysis. Data can also be emailed to outside stakeholders by clicking the Forward button. This attaches the document, file, or ticket to an email and sends it off the system to the selected or entered recipients.

1. Functional structure. The EMIS shall enable approved users to designate groups of users, by name or by functional position.

DLAN administrators can create groups within the system. Groups are flexible and can be used to define a selection of individuals, an organization, department, functional position, etc. Groups can be used to provide security permissions and access to features, or they can be used to identify which groups of users should be able to view an incident, status board, report, folder, file, or document.

2. Incident management. The EMIS shall enable users to manage daily activities and to monitor and track all aspects of an incident or event.

DLAN is specifically designed to support daily operations and emergency response. DLAN provides several tools that can be used daily for normal operations, including event logging, social media monitoring, email monitoring, webpage/RSS feed monitoring, documentation library folders, role based briefing notes, and several other tracking tools. DLAN's robust toolsets will allow users to monitor and track all aspects of an incident or event.

3. Duty and Call Logs. The EMIS shall enable users to access Duty Logs and Call logs.

Duty Logs and Call Logs can be accessed through Ticket Manager Reports. DLAN is often used by Duty Officers to monitor escalating events. It can also be used by call takers as a call center system to log phone calls and information requests. DLAN provides full tracking of logs that are kept by all user positions under specialized ticket reports such as "Tickets Added or Edited By My Role."

4. User management. The EMIS shall enable the system administrator(s) to define roles, assign privileges to users, create, maintain and/or delete users.

Administrators may configure an unlimited number of user accounts, groups, and roles. Groups and roles may be assigned to a user account with a simple checkbox system. Users may have multiple groups and roles if they are trained for multiple positions, this allows them to retain one account and toggle between views as needed. DLAN comes with several default security groups already created, and during the configuration period, BCG trainers will work to create other security groups and user accounts as needed. Administrators can change a user's security permission on the fly and it will apply instantly without the need for the user to log out. This flexible and intuitive security system will cover all your needs and allow system administrators to change or add privilege levels on the fly during an incident. Administrators can also add or delete users with similar convenience.

4.2.1.1.5 Interoperability. Vendor shall provide a solution that could interface with common EMIS web-based solutions.

DLAN is interoperable with EMIS solutions at FEMA Region III States and other Neighboring states out of the box using standard communication and messaging technologies. For additional technical information, please see the response to question 4.2.1.2 above.

1. The EMIS must be fully interoperable with Emergency Management Assistance Compact (EMAC) Operations System (EOS) for all functions.

The DLAN system is interoperable with the EMAC Operations System. Through the DLAN Ticket Manager Premium Module, specifically the preparedness toolkit feature, the system supports EMAC including the planning process, creation, and implementation of Mission Ready Packages using FEMA NIMS Typed Resources.

2. *The EMIS can be integrated and interoperable with the resources management software implemented at the local level, the WVEMD resources management, and EMAC platform, and the Geospatial platform implemented at WVEMD. Currently, the WVEMD uses AssetCloud for managing assets and Inventory Cloud for WVEMD's warehouse items. The Geospatial platform implemented at WVEMD is based on ArcGIS platform.*

Integration with Local Resource Management Software

The system can be integrated with Asset Cloud, Inventory Cloud, or with resource management software used at the local level by agencies, departments or municipalities provided that those systems support standard protocols for data exchange such as links, email, CSV, EDXL-RM, ArcGIS, RSS, CAP, or KML. The system also supports an advanced rules engine interface for integrations that allow WVDEM administrators to automate the evaluation, triage, and assignment of information that comes in from integrated email sources.

Additionally, the system supports integration with these platforms using DLAN system APIs which can be made available upon contract award.

Integration with EMAC EOS platform

The system can be interoperable with the EMAC EOS system, provided that West Virginia is willing to sponsor BCG for that integration project. EMAC requires sponsorship by a State level entity before they will make APIs available to a vendor for interoperability. BCG has not included specific costs for this integration in our price proposal Exhibit A – Pricing.

Integration with GIS

- **ESRI ArcGIS based-** BCG has been providing ESRI based GIS Platforms since 2004 in DLAN. Our proven solutions are fully integrated into our DLAN Incident Management System and allow users to view and work with essential incident information on a map. As GIS software continues to evolve, BCG will continue to set the standard for user friendly incident management tools and fully integrated and interoperable solutions. There are currently two GIS versions available: GIS Basic and GIS Premium.

Visualizing incident data is an essential part of situational awareness, that's why GIS Basic is included in all DLAN systems. GIS Basic provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

- **Ticket Report Sync with ArcGIS** - In addition to incorporating key external data, GIS Premium also displays data from other DLAN modules. For example, resource requests entered into the Ticket Manager appear on the map, as well as other reports and requests. Users can even add and edit tickets directly from the map. Users can also view video from traffic cameras entered into Streaming Video.
- **GIS Premium** -requires a connection to ESRI's ArcGIS Server or an ArcGIS Online account in order to serve up basemaps, provide geocoding & geoprocessing, view data overlay services (layers), use/embed ESRI's operational dashboards into Status Boards, and provide geometry

services. If your agency already has ArcGIS licensing, DLAN can consume and leverage your existing services at no additional cost. DLAN's GIS toolset is compatible with ESRI's ArcGIS Server or ArcGIS Online.

Alternatively, if your agency does not have access to an ArcGIS Server or ArcGIS online, BCG can provide you with access to ArcGIS services. Please talk to your BCG representative for details. Access to BCG's ArcGIS server services includes basic ArcGIS online map services (basemaps, map services, feature services, geocoding services, geometry services, and geoprocessing services). If your agency would like to manage your own custom GIS layers, you will need your own ArcGIS Server or ArcGIS Online account. Additional licensing for custom ArcGIS services is not provided by BCG and is the responsibility of the customer.

3. *The EMIS must have the capability to interoperate with the State's financial administration system to report material transactions including order and receipt of ordered material. Currently, the WVEMD uses OASIS.*

DLAN can export resource reports to common formats such as excel and CSV which can be uploaded into the State's financial administration system. If a more automated approach is desired, BCG could develop a custom integration with the State's financial administration system, however, scope, schedule, and cost, would need to be determined depending upon what software the finance system uses.

4.2.1.1.6 *Reports management. This system shall supply situational reports on the following factors of emergency management: event and incident reporting; resource requesting and management; response inventory management; infrastructure reporting, including road closures, hospitals, shelters, critical infrastructure; damage assessment; Community Lifelines; and a section for documents, images, user directory, organization charts, etc. the situational reports shall be saved as digital format, and printable from the EMIS interface.*

Event and Incident Reporting

The DLAN system provides reporting for individual tasks, missions, and after action reports for emergency events or entire incidents. Reporting on individual tasks or missions (groups of related tasks) is provided through a report generator tool that allows users or administrators to search, use filters, select columns and data, and produce a tabular reports of all important information. Tabular reports can then be visualized as graphs or charts or broken down into statistics using the Stats tool.

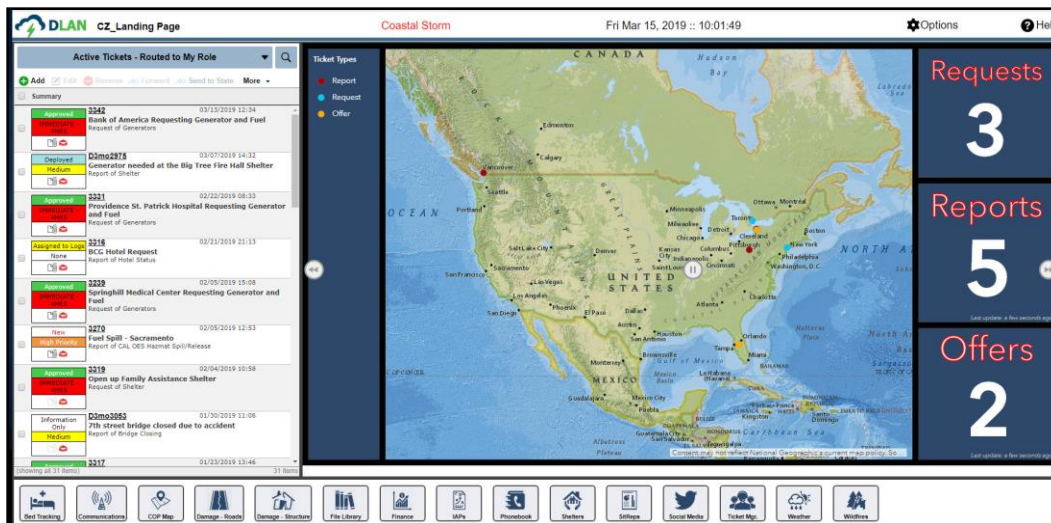


Figure 6: Status Board with Stats

For reporting on the whole incident, DLAN includes an after action report tool that provides customizable AARs that produce a chronological report of every action taken by users during the emergency, including: resource request tickets, situational information update tickets, messages, status board (dashboard) entries, broadcast messages, situation report documents, incident action plan documents, file uploads, reference folder creations, and recorded GIS map screenshots.

Resource Requesting & Management

DLAN Ticket Manager Module allows users to request resources using a simple ticketing system and then routes requests to other roles on the system for fulfillment. A Ticket Wizard option makes entering a request a simple step by step process. Resource requests routed to a user's role will automatically appear on their status board (dashboard) or in their Ticket Manager report. Users can triage request tickets including adding statuses, priorities, attachments, locations, contact information, and other valuable information. As tickets are completed they will fall off of the users' dashboards or ticket reports, keeping information to a focused and management level. Ticket Reports allow users to view completed tickets or information routed to other roles for situational awareness purposes.

Figure 7: Ticket Wizard - Resource Request

Response Inventory Management

The DLAN Resources Stockpile Module will allow WVDHSEM to pre-populate known resources and inventory equipment into the system and assign them to the agency or organization that owns them. This stockpile inventory can then be referenced or searched with the “Find Match” button when entering a resource request ticket. Users entering the request or a user in a logistics role can use find match to pull up the contact record for vendors, suppliers, departments, or agencies that own that type of resource. This makes sourcing equipment a quick and painless process. Stockpile inventory can also be viewed when looking at organization records in the DLAN Phonebook Module to see what resources that organization or agency owns.

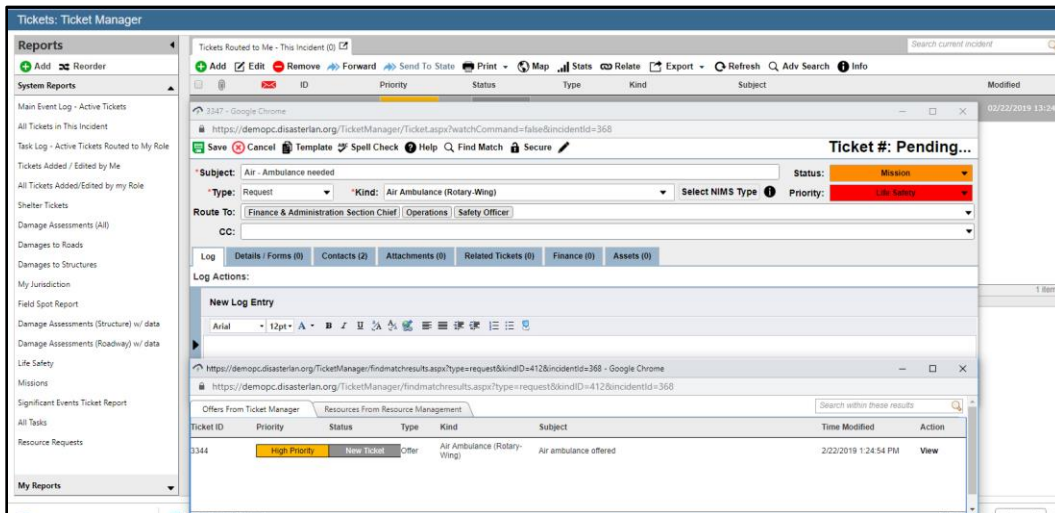


Figure 8: Ticket Manager - Resource Match

The DLAN Assets Module provides further tracking of inventory through the resource deployment, demobilization, and recovery phases of a resource request. Assets allows users to track the specific personnel or piece of equipment that was deployed to the field as part of a request, its current location, its status, images, and other key information on the GIS map. This asset tracking is also integrated right into the original resource request ticket, giving full visibility and accountability to the original requestor and managers that are coordinating resources. The Assets Module can also provide real-time AVL tracking for vehicles equipped with a tracking device or personnel using a GPS tracker. The DLAN Mobile app can also be used to track the location of personnel using the app, provided tracking is enabled on the device.

Infrastructure Reporting

- Road Closures

DLAN’s Status Board Module provides terrific visualization, coordination, and management of key information such as infrastructure reporting in a user focused dashboard. DLAN comes out-of-the-box with a Road Closure Status Board that is designed to populate information automatically from report of road closure tickets or road closure forms submitted from the mobile app. The board includes a tabular view of affected roads with columns for specific road closure data (nearest milepost, northbound/southbound, reason closed, etc.) color coded road status (open, closed, partial, etc.) and a map of the area displaying real-time traffic information from public sources such as ESRI and Google. This board is included with DLAN by default, but can be changed or edited by WVDHSEM as needed to display other real time road closure information.

- Hospitals

Hospitals can be tracked in DLAN Phonebook records which allow users to capture key facility information, resources, personnel, and other data. This can be viewed in the DLAN Phonebook, or in a Status Board (Dashboard) Panel. Additionally, DLAN offers a bed tracking module (not included in the direct cost of this proposal, but available as an option) which offers real time automated and/or manually updated bed status tracking

information, hospital facility capabilities, and bed occupancy information as well as ambulance transport tracking. Bed tracking is based on the Hospital Availability Exchange (HAVE) / HAVBED standard from OASIS.

In the recent past, DLAN has been used to integrate advanced syndromic surveillance report into the bed tracking and GIS map modules to show the top syndromes reported at area hospital ER departments, deviations, trends, ER capacity surges, and warnings related to public health. These integrations were implemented for the Ministry of Health in Ontario to track bed status and facilitate emergency communications between all 350 public hospitals in the Province.

- Shelters

Similar to BCG's Road Closures board, DLAN includes a Shelter board that is designed to pull in shelter information such as shelter name, location, capacity, etc. and display that data in a color coded tabular view in one visual dashboard. Users can edit and update shelter information from the board or submit entries through the Mobile App. As an example, staff on location working at a shelter can update their capacity details and have it sync that information in real-time back to the EOC where it will be displayed on the Shelter Board.

- Critical Infrastructure

The DLAN Phonebook Premium Module will allow WVDHSEM to track critical infrastructure and facilities in a record, capture point of contact information for a responsible person or agency, geolocate the facility to an address or point, and display it in both the Phonebook and on the GIS Map. Facility and infrastructure reports can be created dynamically as needed or pre-built. These reports can be used to color code facilities and infrastructure on the map based on their status (red, yellow, green, etc.). Finally, Assessments (damages, risk assessments, rapid assessments, spot reports, etc.) can be created for each facility and submitted through the Mobile App by field staff going out to do those assessments.

Damage Assessment

The DLAN Mobile Responder App is a flexible multi-purpose two-way communication and information reporting app that runs as a native app on iOS, Android, and Windows devices such as smartphones, tablets, and laptops. The App can be used for a variety of tasks including situation reporting from the field and task distribution, but its primary use case is for completing Damage Assessments and syncing that information back to the DLAN system. The Mobile App has a form based data entry solution, allowing WVDHSEM to design, build, and deploy any form that they wish to a user's mobile device. BCG provides a tried and tested Damage Assessment mobile form that is available out of the box. Users can open the app on their device and fill out a damage assessment on this standardized form. The app will automatically capture the user's location and provides the ability to use the map or an address to adjust it if needed. The app also allows users to take pictures and video and attach them to the Damage Assessment form. When complete, the damage assessment is synchronized back to the DLAN system. If the user does not have cellular or wireless internet connectivity the app will function offline and automatically syncs completed assessments once connectivity is resumed.

On the receiving end, DLAN comes with an out-of-the box Damage Assessment Status Board (dashboard) that populates a report and a map automatically as assessments come in from the field. Incoming damage assessments are automatically converted into actionable damage assessment report tickets and users can manage and update them through the Damage Assessment Status Board or their Ticket Manager page as needed.

Reference Documents

The Reference Library is DLAN's main file storage area and is designed to make files and documents available to staff anytime, anywhere. The Reference Library is not incident specific and designed to store persistent data that needs to be accessible for all incidents, such as policies, procedures, chemical and radiological reference information, emergency evacuation plans, or any other reference document. Three features that differentiate

DLAN's Reference Library from other file storage applications are that it is fully accessible from mobile devices; its intuitive security settings which allow folders to be locked down by the security group to protect sensitive information; and that it can be used to upload any type of file (unless specifically prohibited by an administrator).

The Incident Folders Module is a secondary file storage feature that works similarly to the Reference Library but is designed to save incident specific documentation, such as disaster scene photos, press releases, news articles, static GIS Maps, and agency generated documents. Documents uploaded to the incident folders during an emergency become part of the incident record and after action report. Incident Folders are archived when the incident is archived in DLAN. A pre-set folder structure can be defined and is auto-created for each new incident to create a consistent organizational structure for saving incident specific files. Other DLAN modules have quick-links to store items in Incident Folders or to post documents from Incident Folders to other modules, such as the Status Board. At the end of the Incident, all materials stored in Incident Folders can be downloaded, rolled into a report, or Emailed out.

User Directory

The DLAN User List Module shows which users are currently online/offline and provides a link to message them via DLAN Mail Message (DMail) or Chat message. The User List displays the offline or online status, proper name, username, current role (EOC manager, logistics chief, Red Cross liaison, etc.), Email, and phone number of each user. Users can filter the user list by showing either online or offline users for easier viewing.

Organization Charts

The DLAN Incident Action Plan (IAP) Module enhances the functionality of ICS forms by allowing users to compile them into IAPs following FEMA's guidelines. This includes the ICS 203 and 207 forms for organization charts. An IAP can be published with just the org chart form or as a compilation of any ICS forms that are useful for the current incident. IAP Templates allow users to select a pre-filled IAP org chart that already has key information entered. Or, the user can copy/clone a previous org chart and use it as a starting point for a new one.

- 1. The EMIS shall enable users to access situation reports and visual situation displays, and provide the means for visually presenting situational information in a dashboard and COP.*

The Status Board is designed to display multiple types of situational awareness information in a dashboard format. It leverages both user updated content (e.g. incident messages) and automated external data sources (e.g. Twitter). All content is live and updates continuously for real time situational awareness. All board elements are interactive and the content view can be customized by the user for his or her current session without affecting other users.

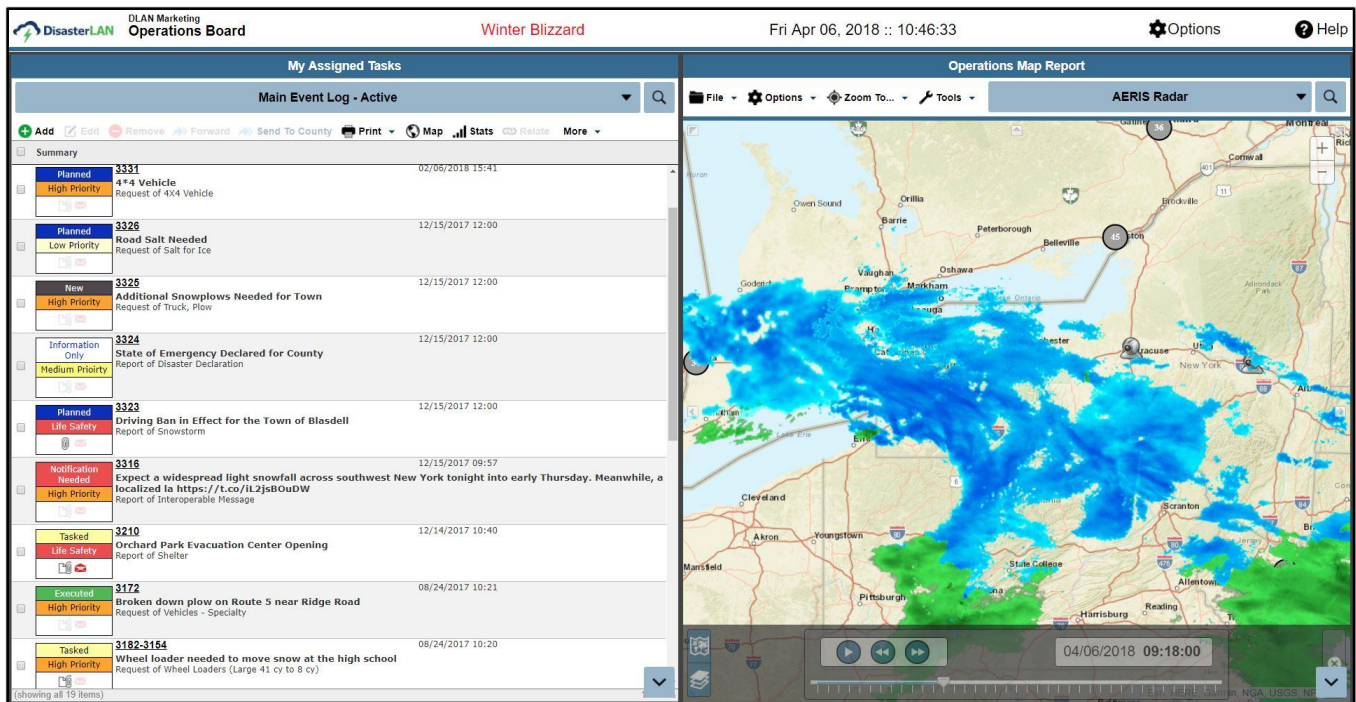


Figure 9: Status Board - Operations

Many subscription (data) types are available to populate each panel. Boards can also display user curated content such as critical decision messages. Boards can be created to display summary or detailed information from multiple incidents in one display. This mixture of different data sources and display types means the number of status boards an organization can make is practically endless, creating a truly customized experience.

The Status Board is specifically designed to be easily viewed on mobile devices, desktops, and projector/television displays. Each individual board panel can be popped out into its own window for full screen viewing.

2. *The EMIS must enable users to access Road Closure Notifications and reports from the West Virginia Division of Highways and display the information in the EMIS solution and the COP.*

DLAN is designed to be interoperable with many common information sharing technologies and can enable users to access Road Closure Notifications and reports from WV Division of Highways and other agencies from within DLAN. Data from 511, National Weather Service, and Twitter can be displayed on DLAN Status Boards. For example, the 511 and WV interstate feeds can easily be displayed. DLAN also supports the display of CAP messages, Atom feeds, GeoRSS, GeoJSON, KML and other sources that can be visualized on the DLAN GIS Premium Map. If none of these existing technologies meets the state’s needs, then BCG can provide a customized integration point using our API.

3. *The EMIS must provide ad hoc user-defined reporting in which dynamic, real-time data reports are created by the user on an as-needed basis.*

Many of the modules in DLAN allow users to create custom reports. BCG's easy-to-use tools allow administrators to lay out new documents, boards, forms, links, and other pages as needed, giving DLAN users a powerful way of managing the various reporting and input needs of each incident.

System reports allow administrators to save reports that are accessible to all users, such as a "completed tickets" report showing only tickets in the incident that have been completed. Users can also create custom reports to show whatever information is of interest to them.

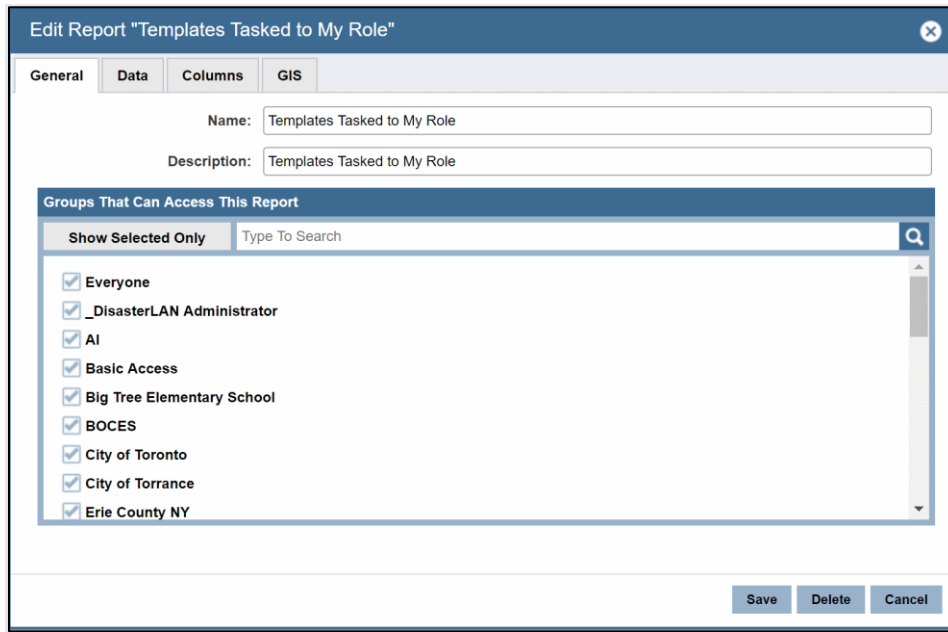


Figure 10: User Defined Reporting

In the Ticket Manager, ticket reports are used to filter the list of available tickets down into meaningful sets of similar tickets so that they can be more easily tracked, worked upon, and completed. Customized views of ticket data (reports, requests, donations, etc.) can easily be queried based on date, time range, incidents, priority settings, status settings, jurisdiction data, user submission data, location data, routing information, keywords, attachment data, and other information. Users can select the columns they wish to see in the report, using any data within the ticket or any dynamic forms created by WV staff. These queries can easily be saved for use by other groups of users in map reports, in ticket manager grids, status boards, or as personal reports. This ability to quickly filter and present data for temporary or permanent use allows the Ticket Manager to be a core data management system for customer displays and views on the system.

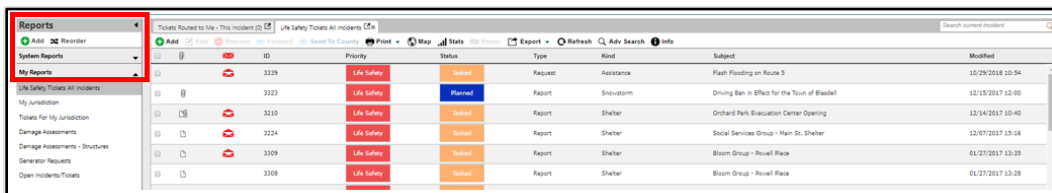


Figure 11: Ticket Manager Report

Like the ticket reporting tools, phone book data can easily be filtered by users to display organizations and people based on filterable criteria such as location, trainings completed, skills possessed, categories, text, and other filters. These reports can then be saved for use by other users on the system in order to easily find contact information on vendors and staff that is specific to their emergency management needs.

Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users.

4. The EMIS must provide data views that users can select based on parameter such as date, event type, counties. The data views should sort those views and enable the user to sort by parameter too.

Customizable views in DLAN allow all users to drill down to whatever data is most relevant to them, including the ability to search sort, sort, filter, and report on all data views.

Grid Views – DLAN ticket information can be easily viewed by selecting parameters the user is interested in. Information can be sorted, searched, and filtered on every data column or entry: such as date, time created, time modified, due date, event type and kind, location, tasking, etc. A simple click on a field or column provides the ability to easily sort and view information in the system. Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users

- Dates – Ticket Information can be sorted and viewed by Last Modified and other date information available on every record.
- Event Type – The event type is captured in the ticket’s Type and Kind fields. The lists are based on NIMS/FEMA types and kinds, but are customizable by West Virginia’s administrators. All this information can be selected and sorted for viewing.
- Ticket Reports – These reports allow custom views of data by user definable parameters such as kind, status, priority, contact information, location, dates, and other information displayed in the ticket.
- The Ticket Manager includes preconfigured forms for capturing additional resource request information and capturing information from off-site staff. It also includes preconfigured reports for easy access to essential information. Additional forms and reports can be purchased individually, or with Ticket Manager Premium you can build your own custom reports and forms.

5. The EMIS must provide detailed user access and activity reports.

DLAN provides detailed user access and activity reports as part of its standard System Administration Site Security reports set - as shown in the illustration below. The User List function will enable Administrators to view and report on all users currently logged into the system. Site Security Reports are also available to provide the following information:

- Currently Locked Out Users
- Currently Logged In Users
- Group Modules
- Module Users
- Portal Users

- Role Association
- Watch Command Activity
- Security Violations
- User Activity
- User Groups/Modules
- User Login History
- User Login Timeline
- User Last Changed Password

The screenshot shows a web-based report interface. At the top, there are input fields for 'Start Date: 3/19/2019' and 'End Date: 3/26/2019', along with a 'Run Report' button. Below this is a navigation bar with '1 of 1' and 'Export to the selected format' options. The main title is 'User Activity Report From: 3/19/2019 11:26:59 AM To: 3/26/2019 11:27:01 AM'. The primary data is presented in a table with columns for Username, Phonebook Entries Added, New Calls Entered (Regular, Watch Cmd), Calls Modified (Add+Edit) (Regular, Watch Cmd), and Total Calls Modified (Add+Edit). Below this is a 'User Activity Summary' section with a smaller table summarizing totals for Phonebook Entries Added, New Users Added, New Calls (Regular, Watch Cmd), Calls Modified (Regular, Watch Cmd), Total New Calls, and Total Calls Modified (Adds + Edits). The footer indicates 'Printed on: 3/28/2019 11:27:01 AM' and '1 of 1'.

Username	Phonebook Entries Added	New Calls Entered		Calls Modified (Add+Edit)		Total Calls Modified (Add+Edit)
		Regular	Watch Cmd	Regular	Watch Cmd	
mward	0	2	1	2	4	6
bcg_cfire	0	0	1	1	1	2
All Users	0	2	2	3	5	8

User Activity Summary From: 3/19/2019 11:26:59 AM To: 3/26/2019 11:27:01 AM		
Total Phonebook Entries Added	0	
New Users Added	0	
New Calls	Regular	2
	Watch Cmd	2
Calls Modified	Regular	3
	Watch Cmd	5
Total New Calls	4	
Total Calls Modified (Adds + Edits)	8	

Figure 12: Sample Security Report - User Activity

4.2.1.1.7 *Geospatial component. The EMIS shall be capable of generating dynamic maps and reports that represent a COP. The system shall be designed and equipped to upload of the GIS information for spatial display in the form of shapefiles, layer files, web map services (WMS), and .kml or .kmz formats.*

BCG has been providing ESRI based GIS Platforms since 2004 in DLAN and in other products. Our proven solutions are fully integrated into our DLAN Incident Management System and allow users to view and work with essential incident information on a map. There is even a mini-map function built into the ticket/task entry screen and preview screens are available if you need to view tasks on a map. Map reports can be created and displayed on a dashboard/status board for easy viewing. Mark up drawing tools and the ability to save or share layers and mark ups is built into DLAN. Users with the appropriate permissions can create maps and reports from the GIS data in the system. As GIS software continues to evolve, BCG will continue to set the standard for user friendly incident management tools and fully integrated and interoperable solutions.

Visualizing incident data is an essential part of situational awareness, that's why GIS Basic is included in all DLAN systems. GIS Basic provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

External data sources for mapping include: Aeris Weather, Aloha Plume, AVL Trackers, CAD data via Email or custom API, CSV, Drone Imagery, ESRI ArcGIS services, ESRI Online services, Excel, GeoJSON, KML, WebServices and Shapefiles.

DLAN Module mapping data sources include: Asset Tracking Reports, Incidents & Events, Mobile Responder Phonebook Premium Reports, Phonebook Reports, Risk & Resiliency, Route Analysis, Streaming Video, Ticket Manager Premium Reports, Ticket Template Layers.

DLAN GIS works with ESRI's ArcGIS Server or an ArcGIS Online to serve up basemaps, provide geocoding & geoprocessing, view data overlay services (layers), use/embed ESRI's operational dashboards into Status Boards, and provide geometry services. If your agency already has ArcGIS licensing, DLAN can consume and leverage your existing services at no additional cost. DLAN's GIS toolset is compatible with ESRI's ArcGIS Portal/Enterprise or ArcGIS Online.

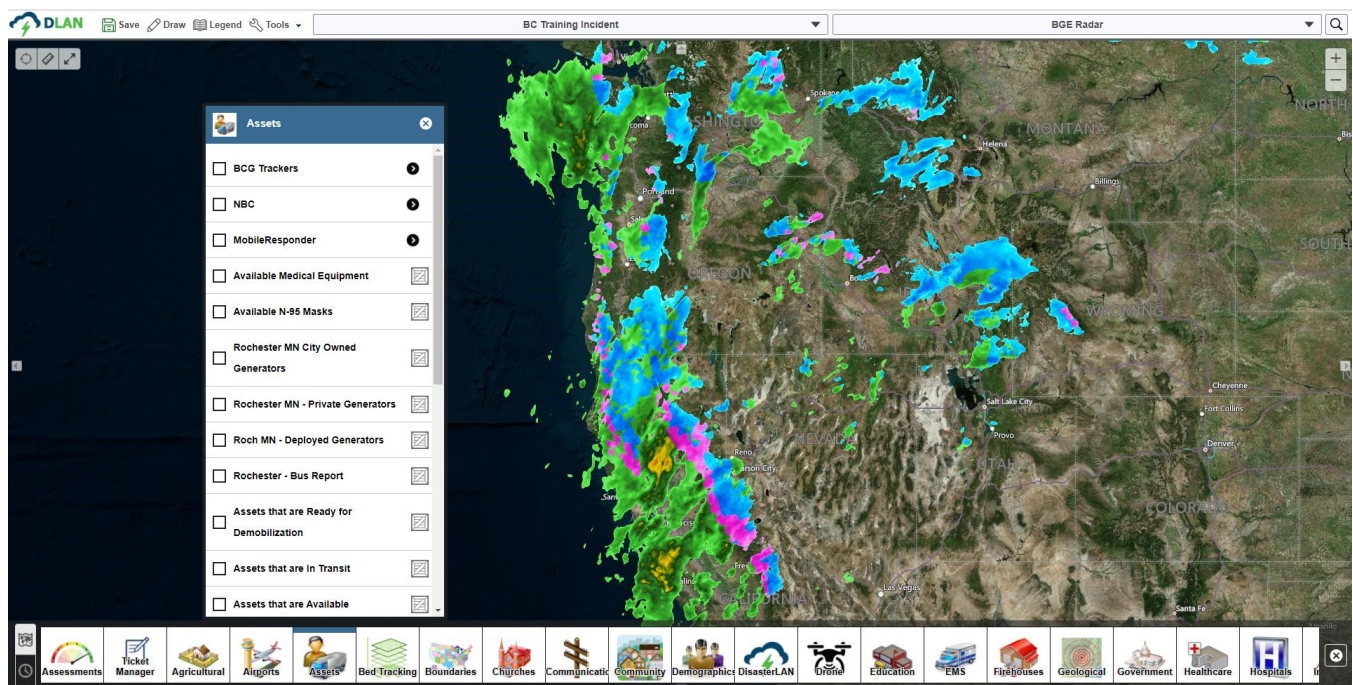


Figure 13: GIS Map Spatial Displays

1. *The EMIS's geographic component shall be capable of displaying a dynamic map identifying incidents, events, effects related to those events: and, the responding agencies involved, including agency contact information.*

All Incident and event can be illustrated on a GIS map in the system. The data that includes GIS information can be displayed and edited on a dynamic map. Additionally, as users interact with the system and add content such as incidents, events, effects, and responses/comments, the system automatically builds GIS layers out of that content which are visible on the GIS map and update in real time as users update the content. Examples include: incidents, events, tickets, facilities/organizations, personnel, assets and resource locations, assessments, weather data, streaming video, templates/mission packages,

2. *The EMIS's geographic applications shall allow users to add new layers to the dynamic map.*

GIS Administrators will have full access to the admin menu, which will allow them to customize features such as basemaps, overlays, layers, and categories.

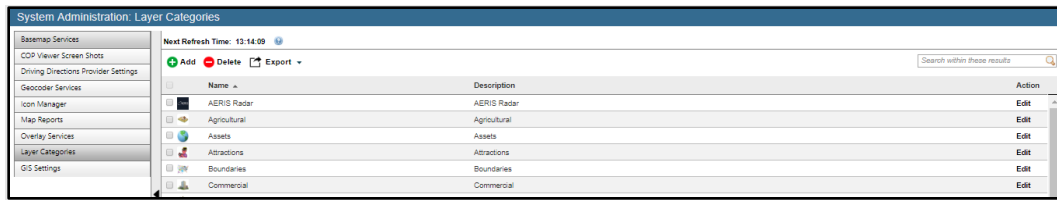


Figure 14: GIS Admin

3. *The EMIS's geographic application shall permit users to use the geographic analysis functions.*

DLAN's GIS module allows users to use a variety of geographic analysis tools and reports such as proximity indicators, finding the nearest point, and creating buffers to estimate possible human, property, and infrastructure effects. Additionally, the EMIS is integrated with ArcGIS products and can leverage the numerous powerful geographic analysis functions available through the ArcGIS platform. Any analyzed data can then be synced back into the DLAN EMIS system.

4. *The EMIS shall enable the user to edit and update layers, query multiple datasets, and export the query in GIS formats, tabular or delimited formats.*

GIS data can be organized into categories that appear on a touch-screen friendly ribbon, making location and toggling layer information on and off a snap. Additionally, data layers can be locked down to select users based on administrator configuration. The system supports the sharing and export of GIS layers and data to external recipients (outside of the EMIS) as CSV exports or KML.

5. *The EMIS's geographic component must have a geographic application capable of supporting the resource request management.*

DLAN provides all the tools necessary for the display and visualization of resource requests and supplies within the GIS Module. Maps can be used to display resource request locations. The mapping tools also allow the ability to view the status of resource requests and delivery locations of resources on either a map or table. Figure 3: GIS Map Requests and Reports displays a snapshot of a resource deployment ticket being updated directly from a Resource Location map. This solution also supports tracking of personnel resources through the mobile app with real time GPS tracking available on the GIS map for safety, tracking, and search operations.

6. *This geographic application shall contain dynamic maps for displaying information such as the status of resource request and delivery location. The dynamic maps must deploy in real time the resource request status on a map and in a table view. The application shall permit add, remove, and edit layers.*

DLAN's GIS dynamic maps and mapping tools allow the user to view the status of the resource requests and delivery location on either a map or table. GIS information is displayed in real time and includes the ability to automatically record changes in the GIS map from both user input data and automated data feeds. Data can be organized into categories that appear on a touch screen friendly ribbon, making location and toggling layer

information on and off a snap. Additionally, data layers can be locked down to select users based on administrator configuration.

Data for Resource Requests including status are visible in a table view in the Ticket Manger module and in a GIS map view as a layer in the GIS Map module. A WVEMD administrator can add, remove, and edit layers as needed through the system administration pages. All changes are reflected in real time.

7. The EMIS shall permit dynamic search by address, toponyms, coordinates, and resource type. The application shall work on computer, tablet, and mobile devices.

DLAN's GIS Mapping tools and search dynamics allows users to search by address, toponyms, coordinates, and resource type. All table views / data grids in the system can be searched and sorted and will return any data that appears in the table. Additionally, all areas of DLAN, including the Map and dashboards scale to work on desktop computers, laptops, tablets, and mobile devices.

8. The EMIS's geographic component must include and integrate mobile applications to collect, present and disseminate data and information.

With DLAN's Mobile Responder App, emergency managers in the field can easily communicate essential information with each other and back to the EOC using their mobile devices. The App is designed for disaster area use and can function regardless of connectivity. The simple form interface makes the app ideal for data collection- including damage assessment, debris management, and spot reports from field staff. Using the Mobile Responder, users can send data, images, and videos from their mobile devices into DLAN.

Once a form is received by DLAN, it can be reviewed and posted to a ticket or submitted to the Risk & Resiliency Module. Alternatively, mobile forms received by DLAN can be posted to a ticket automatically based on business rules. This gives users the power to then run reports on damages, map locations, and assessment information and share it with interested parties within or outside of the EOC with no need for double data entry or phone calls.

Offline Functionality

The Mobile Responder App allows field staff to work offline with any mobile form on their system. The App stores all report data locally on the device and automatically sends it to DLAN whenever connectivity is reestablished. This "store and forward" capability ensures data integrity and usability under the most adverse conditions.

Assigned Task Mode

DLAN simplifies the user experience by focusing their attention on only the tools they need to do their job. The Assigned Task Mode in the Mobile App helps get field workers started on their daily duties quickly. The App can now automatically sync and download all the tickets assigned to a field worker (routed their role) when they first log into the app. This includes all information the field worker needs to do his or her job, including forms, basic ticket data, and contact information for the person who assigned them the task as well as contacts for the job

location and anyone else assigned to assist on the task. Additional tasks can be pushed to a field worker in real time and completed ones will synchronize to DLAN when published. If the field worker enters an area with no cellular or wireless connectivity they will still have all their assigned task data to work with offline. When the worker returns to an area with connectivity, the App automatically publishes their completed assignments to DLAN.

The Mobile Responder App is included in our DLAN Advanced and Premium editions, as well as in all of our industry packs; it can also be added to any DLAN System as an option. The App can be downloaded for free from the Apple App store and Google Play store; authorized DLAN credentials are necessary to use the App.

9. The EMIS must enable users to track incident locations and information and develop trend data over time during and incident.

As the record changes in the GIS map from both user input data and automated data feeds; it also snapshots an image of the map change, and saves it to the incident record. This allows WVEMD to review what the historical map looked like at point throughout the incident, and justify or reconfirm any decisions made based on geospatial situational awareness. Authorized users can view a chronological record of geospatial changes throughout the incident to help identify trends.

4.2.1.1.8 Training. The vendor shall provide all training opportunities leverage against the State's development and training platform of the EMIS solution. The vendor shall provide training for:

BCG can perform all training and exercises using the State's DLAN Development or Test Site. The Development Site can also serve as a test bed for new releases and updates so that the State can test them in a controlled environment before applying the update to the production EMIS site.

1. Users.

BCG will provide onsite instructor-led basic user course training for these users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

2. Trainers.

BCG will provide basic, advanced, and administrator course training for these users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

3. System Administrators.

BCG will provide administrator course training for these individuals. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

4. Technical Staff, to include Information Technology, Programming, and GIS staff.

BCG will provide a technical training for these users. BCG will also provide necessary knowledge transfer during project implementation to assist these technical users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

4.2.1.1.9 The Vendor shall make training available on-site for all user levels. The vendor shall identify the following:

BCG will make training available at the State for all levels of users of the DLAN EMIS as part of the EMIS project implementation. BCG trainers are not just experts in the technical aspects of the system, but also in its applications in emergency management. All our trainings will be tailored to WV's specific organizational workflows and DLAN site configuration

1. Course names (Serialized and in Sequential organization order)

Onsite, instructor led training broken down into:

Administrator Training

- General DLAN Functionality overview
- New Incident Creation
- User & Role Management
- Security Groups and Record Security
- System Setup and Configuration
- Module Administration
- Status Board Building
- Form Building
- System Reports Creation
- Workflow Creation

Basic User Training

- Introduction to DLAN
- Login & Navigation
- Landing Pages and Status Boards
- Ticket Wizard
- Ticket Manager
- Mobile App
- Communication Center
- GIS Mini-map
- Calendar & User List
- IAPs, Phonebook, Resources, & Assets
- Ticket Manager Premium, Templates
- Resources & Assets
- Communication Center External Messages
- Status Board Content Curation
- IAP Creation
- Situation Report Creation
- GIS Premium Map Viewer
- User Reports Creation

Training Materials Provided:

- Training Agenda for basic, advanced, and administrator training courses
- Training Quick Reference Guides for all DLAN Modules owned by West Virginia
- PowerPoint or Video Recording of training courses

Additional training resources included:

- DLAN Online Help Articles
- DLAN Reference Library Materials (storage for all current quick reference guides and training materials)
- DLAN In-Board Help (Situation Report Builder Board & IAP Builder Board)

2. *Delivery Methods*

Training delivery methods typically include onsite instructor led training using a mixture of lecture and hands-on activities where students perform operations and exchange data with others using the DLAN software. Training can be delivered either virtually or at WV's facility of choice.

Alternative services: BCG can provide virtual trainings, webinars, one-on-one coaching, train the trainer sessions, custom training videos, and custom training documents to meet West Virginia's specific needs.

3. *Length of each course*

The DLAN Administrator Training Course is designed to run two full days for a state level system. Time may vary slightly depending upon the number of modules and features included in the State's DLAN system.

The DLAN Advanced User Course typically runs one day.

The DLAN Basic User Course is designed to run one full day session based on the number of modules and features included for Basic Users in the State's DLAN system as well as the group size. BCG will run multiple basic user training course sessions over a two-day period to accommodate larger audiences and ensure all staff is trained. Users only need to attend one session.

5. *Schedule for standard yearly training course.*

BCG can provide DLAN Refresher Training on a yearly basis. Refresher Training consists of condensed versions of the administrator, advanced, and basic user training courses as well as coverage of new features and functionality introduced over the last year with DLAN system updates. If annual onsite instructor led training is not the best approach for the State based on the number of users to be trained or their geographic dispersal, BCG can provide an alternative solution such as online webinar or video based training as a yearly refresher course. For several clients, BCG also develops and runs tabletop or full scale exercises annually as part of their refresher training.

6. *Type of course material that will be provided (course handouts, presentations, and other training materials).*

- DLAN Training Agenda (Training Plan) for Basic User Course, Advanced User Course, and Administrator Course.
- DLAN Quick Reference Guide Documents (Training Materials) for Basic User Course, Intermediate User Course, and Administrator Course.

- DLAN Training Course PowerPoints or Recorded Video of Trainings for Basic User Course, Intermediate User Course, and Administrator Course.

6. *Methods of ongoing, continuing, and on demand training.*

Online Help – The DLAN system includes a built-in online help system that features approximately 375 articles that cover all aspects of the software’s use and functionality with text, images, and step by step instructions. The help system is context sensitive, ensuring that when a user clicks the help button he or she is directed to a relevant article based on the feature or page with which the user was interacting. The help system works with both an online and offline connection. The help system serves as a real-time updated user manual and fosters self-paced learning and as a training refresher on system functionality.

In addition, BCG Support’s Help Desk is available 24/7 and BCG will provide two days of onsite instructor-led DLAN refresher training per year. And you can also schedule new release review webinars on demand with knowledgeable BCG Test Engineers and QA staff.

4.2.1.1.10 *The Vendor shall provide initial training on-site for the following users. This training must be accompanied by user manuals.*

1. *System Administrators to include user access management, a minimum of ten (10) users.*

BCG will provide 2 days of onsite instructor led system administrator course training. BCG will provide administrator training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

2. *State Agency representatives, a minimum of fifty (50) users.*

BCG will provide 2 day of onsite instructor led advanced user course training for state agency representatives. BCG will provide advanced user course training documentation in the form of quick reference guides. Documentation will be delivered electronically.

3. *Local Jurisdiction representatives, a minimum of two hundred (200) users.*

BCG will provide up to 4 total days (shared with NGO training) of onsite instructor led basic user course training for local jurisdictions and NGOs. The days of training will be broken up into multiple sessions. Users will only need to attend one session. Session length is variable based on the number of users to attend, but is typically 4-8 hours depending on group size and the configuration of the state’s DLAN site. This training will be shared between Local Jurisdictions, NGOs, and break-out sessions for technical staff who are expected to have a similar level of access. BCG will provide basic user training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

4. *Non-governmental Organization Representatives, a minimum of one hundred (100) users.*

BCG will provide up to 4 total days (shared with Local Jurisdiction training) of onsite instructor led basic user course training for NGOs and local jurisdictions. The days of training will be broken up into multiple sessions. Users will only need to attend one session. Session length is variable based on the number of users to attend, but is typically 4-8 hours depending on group size and the configuration of the state’s DLAN site. This training

will be shared between Local Jurisdictions, NGOs, and break-out sessions for technical staff who are expected to have a similar level of access. BCG will provide basic user training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

5. Federal Agency Representatives, a minimum of twenty-five (25) users.

BCG will provide a tutorial Video-based training course for Federal Agency Reps that is designed to provide a self-paced learning path for Federal Reps. Documentation will be delivered electronically. These users are expected to have an observer level of access and should need limited training. However, Federal Reps who need or desire a higher level of access can attend the basic user training course.

4.2.1.1.11 Document Management. The EMIS shall offer a document management component to support the emergency management workflow.

The DLAN Reference Library and Incident Folders Modules provide document management features for users and administrators.

Reference Library- The Reference Library is DLAN's main file storage area and is designed to make files and documents available to staff anytime, anywhere. It is included with our DLAN Advanced and Premium editions and can be added to any DLAN System. Unlike DLAN's other file storage area, Incident Folders, the Reference Library is not incident specific and is designed to store persistent data that needs to be accessible for all incidents, such as policies, procedures, and emergency evacuation plans. Three features that differentiate DLAN's Reference Library from other file storage applications are that it is fully accessible from mobile devices; its intuitive security settings allow folders to be locked down by security group to protect sensitive information; and that it can be used to upload any type of file (unless specifically prohibited by an administrator).

Incident Folders- The Incident Folders include all of the features of the Reference Library, but is designed to save incident specific documentation, such as disaster scene photos, press releases, news articles, agency generated documents, reports, and ticket information. With Incident Folders, each incident has its own set of incident folders. The structure of these folders can be pre-defined to create a consistent organizational structure for saving incident specific files. Like the Reference Library, security can be set for each individual folder, so that only authorized security groups will have access to the information. Other DLAN modules have quick-links to add items to Incident Folders and items in the Incident Folder can also be posted to other modules, such as the Status Board. At the end of the Incident, all materials stored in Incident Folders can be downloaded, rolled into a report, or Emailed out. Incident Folders are included with our DLAN Advanced and Premium editions and can be added to any DLAN System

1. The EMIS shall enable users to access procedures, check lists and organization charts, and other documents.

DLAN's Reference Library provides easy access to plans, procedures, checklists, organization charts, and other documents. Documents stored in the Library can be shared, secured (visible only to authorized users), and posted

to dashboard as needed. Additionally, the DLAN Incident Action Plan & ICS Forms module support the ICS 207 organization chart form which can be filled out saved, shared, and posted.

2. *The EMIS must allow users to import and export information including resource data.*

DLAN allow users to import and export information such as resource data through standard tools. Resource data as well as any other data tables can be exported using the export button (CSV, Excel, Word, PDF, etc.). Reports and documents can be shared via email and other methods to internal users or external sources. Files such as GIS files can be downloaded as KML, Shape, or CSV files.

3. *The EMIS shall enable users to prepare and disseminate situation assessment information and recommendations.*

DLAN allows users to prepare and disseminate situation assessment information and recommendations to both internal and external stakeholders through the Situation Report module. Agency Reports can be submitted by the roles responsible, the Situation Report document can be compiled by the planning section or a relevant position. Finally, the individual reports or the Sit Rep can be viewed in DLAN, forwarded out to stakeholders via email, or posted to a Dashboard for consumption as situational awareness information.

4. *The EMIS shall provide access to electronic West Virginia Emergency Operations Plan, State Emergency Operations Center (SEOC) Standard Operating Guidelines (SOG), Incident Command System (ICS) forms, documents, and templates for approved user to edit, update and subsequently store within the application in the user interface.*

DLAN will allow approved users to edit, update, and store documents and templates within the Reference Library Module of the system. Please see (4.2.1.1.11) for more information on this module.

5. *The system must also provide for customization of displays or reports, based on the users' needs*

DLAN is a highly configurable system designed to make filtering of data easy for users. There are numerous ways that customized views, dashboards, landing pages, status boards, and reports can be created on the system. The following are just a sampling of the many ways that displays and views can be customized by users:

- **User, Role, and Task Based Status Boards** – Customized views can be created out of any of the modules and situational awareness panels on the system to allow for user, role, and task specific views to be created and re-used on the system. These dashboards can also be set as a user's or role's landing page (homepage) in the DLAN system. Combined with Workflow Mappings, this presents a completely tailored user experience for each federal or state agency, local jurisdiction, NGO or other organization on the system.
- **Customizable Ticket Reports** – In the Ticket Manager, ticket reports are used to filter the list of available tickets down into meaningful sets of similar tickets so that they can be more easily tracked, worked upon, and completed. Customized views of ticket data (reports, requests, donations, etc.) can easily be queried based on date time range, incidents, priority settings, status settings, jurisdiction data, user submission data, location data, routing information, keywords, attachment data, and other information. Users can select the columns they wish to see in the report, using any data within the ticket or any dynamic forms created for or by WV staff (i.e. damage assessments, debris clearance forms, sheltering forms, etc.). These queries can easily be saved for use by other groups of users in map reports, in ticket manager grids, in

status boards, and as personal reports. This ability to quickly filter and present data for temporary or permanent use allows the Ticket Manager to be a core data management system for customer displays and views on the system.

- **Customizable Phone Book Reports** – Like the ticket reporting tools, phone book data can easily be filtered by users to display organizations and people based on filterable criteria such as location, trainings completed, skills possessed, categories, text, and other filters. These reports can then be saved for use by other users on the system in order to easily find contact information on vendors and staff that is specific to require emergency management needs.
- **Filterable Grids** – Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users.
- **Map Reports** - In addition to the dashboard, landing pages, and situational awareness views that users can create, Map Reports can be used to display specific map information. GIS administrators can configure map reports including basemap and layer settings to be viewed in the COP Viewer or as part of the Status Board.

6. The EMIS must generate reports as requested on the levels of material at the report time and usage or consumption over a defined time interval to enable consumption to be addressed.

The DLAN Resources Module provides a view of all resources used during the incident. It can be searched or filtered by NIMS Type, Category, or Location. The Resources Module provides several standard reports that can be generated as needed. These include a master resources inventory list, detailed organization resource inventory list, and summary organization resource inventory list. User can track material levels, usage, and stockpile levels for each resource kind.

7. The EMIS must be able to receive, record and log incident intelligence and security reports from identified and verified external agencies

DLAN can log intelligence and security reports from external agencies through the use of the DLAN Mobile Responder App. External Agencies can use the app to submit an incident intelligence report, security report, or any other type of information. This information is filled out on the app using customizable forms. When saved, the data is synchronized to DLAN in real time and populates a Status Board with the relevant information. It can also populate tickets and trigger notifications and alerts.

8. The EMIS shall be capable of storing and managing documentation to be retained as record.

DLAN is an audit ready system that automatically logs all historical data. In addition to retaining official documentation, DLAN will allow administrators to run incident reports. Incident reports are comprehensive chronological reports detailing all additions and modifications to records and data that occurred during an incident or event. Reports can be filtered down to a specific date range or type of records, including tickets, messages, broadcasts, Status Board items, uploaded Incident Folder Documents, Situation Reports, ICS Forms, Incident Action Plans, and GIS Map Snapshots. Like other DLAN reports, the Incident Report can be exported or printed as needed.

9. *All data shall remain the property of the state and will not be available for dissemination by the vendor.*

All data entered into DLAN will remain the property of West Virginia and will not be disseminated by BCG.

4.2.1.1.12 *Logistics support. Resource management. The EMIS shall enable users to direct, task, receive, and monitor resource requests.*

DLAN's robust Ticket Manager System and the integrated Resource Request functionality provides concise logistical support within the system. It allows users to direct, task, receive, and monitor resource requests.

Standard Resource Request - The Resource Database is DLAN's main resource inventory portal. It provides a way to enter, manage, and track supplies and resources. Resources can be added to organization records to establish suppliers and inventory stockpiles. They can also be automatically matched to tickets in the Ticket Manager making fulfilling resource requests quick and easy. As resources are added to the resources stockpile or deployed for use during an incident, the list of available resources can be updated accordingly, giving an accurate, real time listing of available resources. It is included with our DLAN Advanced and Premium editions and can be added to any DLAN System. Tickets with resource requests can be routed to specific users for fulfillment.

Standard Resource Forms and Reports include: Request form, and Field report forms.

The Ticket Manager is DLAN's main resource, issue, resource and task management module and is included in all our standard editions. It creates a common area for collaborative issue tracking, initial resource requesting and real-time information sharing using straightforward color-coded statuses and priorities. The Ticket Manager provides user-friendly data entry tools to make logging and tracking critical information quick and easy. It allows both task and mission information to be entered, prioritized, routed/assigned, and followed from start to completion. The Ticket Manager includes preconfigured forms for capturing additional resource request information and capturing information from off-site-staff. It also includes preconfigured reports for easy access to essential information. Additional forms and reports can be purchased individually, or you can upgrade to Ticket Manager Premium to gain access to DLAN's custom report builder.

1. *The EMIS shall enable users to plan and manage the acquisition and distribution of personnel, equipment, and material required to sustain an incident operation.*

Logistics support users can triage and manage resource requests, personnel requests, acquisitions, equipment and other materials related to an incident. The Find Match button allows them to match up a request ticket with a stockpile resource or vendor. The Assets Module, allows logistics support users to track equipment assigned to the field including its current location and status (e.g. en-route, on-location, ready for demobilization, etc.). This type of logistics function is an area where DLAN truly excels above other EMIS software through its Ticket Manager, Resources, and Assets functionality.

2. *The EMIS shall enable users to register, update, and delete resources from the resource management component.*

DLAN's resources module functionally allows users to register, update, and delete resources from the resource stockpile and management ledger as needed. The ability to do so is security controlled based on permissions.

Additionally, users can request, update, and offer resources through the Ticket Manager's resource request and management features.

3. The EMIS shall offer a resource request option with the capacity to document partially fulfilled requests.

The Resource Request tickets entered into the system by users can be routed (assigned/shared) to one or more roles or positions. Multiple users, liaisons, and other contributors can partially or fully fulfill the request. Resource request questions and additional information can be collected on the request form and notes from participating agencies, liaisons, and users are tracked in the log notes. Once resources or equipment are deployed to the field the assets tab of the ticket tracks the individual fulfillment, status, and location of each resource individually as a sub-component of the request ticket.

4. The EMIS shall enable users to track the pre-positioning of resources and managing supplies in facilities.

The DLAN Phonebook allows logistics support users to build out vendor, organization, and facility records including what resources are owned by that organization or currently located at that facility. This is especially useful when setting up staging areas and forward command posts. These records can be populated ahead of time and displayed on the DLAN GIS Map for geospatial planning and analysis.

5. The EMIS shall enable users to task transportation resources to transport and deliver supplies.

The DLAN Ticket Manager module is designed to allow users to task out responsibility for an action to another role. Logistics users can receive a resource request ticket, source the equipment, and then route the ticket forward to a transportation role for delivery of the supplies. Each role plays their part in completing the ticket. At each stage notes and actions are logged, the ticket status is updated to reflect its current spot in the process, and users are alerted when a new ticket lands on their dashboard or report.

6. The EMIS shall enable users to monitor and forecast the consumption of supplies.

The DLAN Resources Module allows logistics users to decrement known stockpile resources as they are consumed so that additional supplies can be sourced when stocks get low. Additionally, the Statistics feature allows user to view resource request tickets broken out by type, kind, role responsible, and other trends so that users can forecast future supply needs.

7. The EMIS must allow users to plan, manage, track, and observe costs incurred.

The DLAN Finance Module provides the necessary tools to help users and administrators track costs for missions, tasks, and resources. It is based on FEMA's reporting standards and can also be configured to the state's needs. Finance records can be entered either from the finance tab in a ticket or through the Incident Ledger page. Each finance item is associated with a particular incident and with a ticket that tracks the finance request and its current status. DLAN comes pre-loaded with a resource list and cost codes that are based upon FEMA's equipment list costs. Custom resource codes and costs can also be added by an administrator. Information about the item, delivery info, wage info, and invoicing are all recorded by the system.

8. *The EMIS shall provide users electronic and printable forms for logging and reporting the ordering, receiving, and issuance of material.*

Asset Tracking provides a way for users to track deployed assets and resources for a particular incident and quickly view the status, quantity, and location of all deployed assets in the asset ledger. All forms and reports can be printed.

The screenshot shows a web-based form titled "Edit Asset". The form has a blue header with a close button. The fields are as follows:

- Item:** Snow Blower (8580) - 2,000 tph - 400HP
- Description/Notes:** Small Snow Blower
- Serial Number:** 321654987
- Quantity:** 3
- Resource Provider:** International Relief
- Obtained:** Stockpile
- Transporter:** Highway Department
- Status:** On Scene / Deployed (highlighted in red)
- Ticket ID:** 3182-3178 - Move snow at high school. A warning below reads: "Warning: changing Ticket ID will permanently move these assets to this ticket".
- Label:** (empty)
- Location:** Lat N42°47'45.77" Lon W78°50'41.39". Below this, it says "Geocoded as: POINT(-78.84483 42.796048)".

At the bottom right, there are three buttons: "Save", "Delete", and "Cancel".

Figure 15: Asset Form

9. *The EMIS shall receive, log and report to users the status of personnel, equipment, and logistics resources throughout an event.*

Reports can be created within the system and made accessible by authorized users/teams on the real time status of all resources throughout an event. This feature is included in the Ticket Manager Premium Module. Once created, a report can be added to a Status Board for visual display and sharing.

10. *The EMIS must enable logistics support users to plan and monitor the routing and movement of supplies from staging areas, distribution points, and other supply facilities.*

DLAN supports supply chain logistics and transit of vehicles, equipment and supplies through the use of the Assets and GIS Modules. Logistics support users can plan a route on the map, mark it up, and share it with other agencies or parties as a static map image, interactive map report, or as a downloadable KML file. If West Virginia has GPS tracking devices that they use on their equipment or vehicles (ex: magnetic slap and track devices), those can be integrated and displayed on the GIS Map. The DLAN Mobile Responder App can also be used as a GPS tracking device. This allows vehicle operators transporting supplies to download the app (free from the app store) and they can be tracked in real time in DLAN.

11. *The EMIS must enable logistics support users to monitor and manage stocking levels of supplies held in staging areas, distribution points, and other supply facilities.*

The DLAN Resources Module is designed to allow users to pre-populate DLAN with known supplies and resources along with their location and contact person/ordering information into a known "Stockpile." Each supply depot facility can also be entered into DLAN as a record and displayed in resource reports, phonebook contact reports, and on the DLAN GIS Map. This provides three ways to monitor and manage stocking levels. Additionally, the Resources Module allows users to decrement and track quantity, cost, and other basic supply information.

12. *The EMIS must be capable of allowing accessibility on mobile devices in an application format. Mobile applications shall be able to perform all functions of basic inventory management without the need for data connectivity due to potential lack of communications in remote sites. Mobile applications shall be able to perform automatic inventory updates when a user enters into an area that has data connectivity available.*

DLAN does have a mobile app that has versions for Apple, Android, and Windows devices. The Mobile app can be used to perform basic inventory management tasks without the need for data connectivity, and will automatically sync the data when a connection is available. For example, a user can submit a resource request from the field and have it sync to the system for management and fulfillment. Additionally, updates and assignments can be pushed from the web interface down to the individual mobile device of a user who is responsible for the information.

13. *The EMIS shall be capable of supporting hardware such as barcode/QR Code scanners and barcode/QR Code printers. Mobile applications shall be capable of utilizing the mobile device camera as a barcode/QR Code scanner.*

The EMIS is capable of supporting hardware such as barcode/QR Code scanners and printers. For example, DLAN users can add QR codes to Status Boards and documents that can then be scanned using a phone or device to prompt an action such as accessing an executive summary report, linking to other sites for additional information or briefings, etc. Mobile devices can scan bar codes or QR codes using the camera on the mobile device. Images of Bar codes and QR codes can be captured using the app and attached to submissions.

4.2.1.1.13 *Financial and administrative support. The EMIS shall provide support for the following processes:*

4.2.1.17.1. Identify material and personnel that require payment.

The finance tab in a DLAN ticket can be used track the material, personnel and required payments associate with a finance cost. The ticket's statues can be used to track payment progress and can be adjusted as a cost moves through the system. For example, the ticket status may be set to Procurement Needed, Approved, Payment Pending, Paid, Reimbursement Pending, etc. These statuses are configurable by a system administrator.

The DLAN Incident Ledger page also provides data for reimbursement payments including 25% and 75% reimbursement rates and total sums.

4.2.1.17.2. Enter and record all cost data.

The DLAN Finance Module does allow users to enter cost data, and that data will be saved and easily accessible.

4.2.1.17.3. Maintain accurate records of incident costs.

The DLAN Finance Module's Incident Ledger feature allows users to quickly generate custom reports about financial items for the current incident. All finance pages support searchable and sortable data columns, exporting data to Excel, Word, or CSV files, and automatic subtotaling and totaling sums. This means that the current spend level for the incident is always totaled and available.

4.2.1.17.4. Support planning activities through preparation of estimates for resource usage.

DLAN supports planning activities including the preparation of estimates and expected resource usage through the use of the Preparedness Toolkit features. This functionality allows an authorized user or administrator to prepare templated tickets ahead of time for common resource requests and standard mutual aid requests such as mission ready packages. These templated tickets can include all financial information and costs relevant to equipment and personnel involved with the task or mission. Templated tickets can be activated individually or in bulk (mass activated) by an administrator as needed. Templates can also be used by basic users as a way to enter a standardized ticket with pre-filled information in a quickly and accurately rather than building a resource request ticket from scratch. Finally, templated tickets are associated with a scenario/incident category and can be automatically activated when an incident of that type is created. This provides an immediate action plan and important tasks at the beginning of an incident response when time is most critical.

1. Financial and administrative support for procurement of material and services.

The Finance Module provides all necessary information to track procurements, purchase orders, receipts, and payment information for materials and services. Finance information is viewable in a tabular page or on a dashboard or mobile device.

2. Monitoring and reporting of costs related to an incident.

All costs associated with an incident are tracked in the Finance Module. This includes individual line items for resources, equipment, personnel, and services with quantity, unit costs, and expected total costs. The Finance Incident Ledger also automatically totals all running costs for the incident so that the State knows when their obligations are met and when federal will become available. The Finance Module also allows finance users to create configurable reports to get detailed information on specific resource types, categories, purchase orders (with multiple items), vendors, statuses, date filters, and DRP eligibility.

3. Providing cost analysis services.

DLAN's Finance Module is designed to track all costs and display running totals for each task, mission, and the incident as a whole. Customizable finance reports help with analyzing trends. DLAN also tracks displays promised payments, payable by, and expected costs as well as delivery,

wage info (normal/overtime), and invoicing information. With all this information in the system, the backup data for reimbursement is simple and at the state's fingertips.

4. *Documenting individual transaction receipts.*

DLAN's Finance Module does save all transaction history, no matter how small.

5. *The EMIS must enable users to provide administrative support for procurement of materials and services including the ability to:*

1. *Identify local sources for equipment rentals.*

The Find Match feature in the DLAN ticket matches a resource request entered by a user with a known supplier of that type of resource. It matches a request ticket with a resource record and phonebook contact for the supplier. This includes equipment rental services.

2. *Identify local sources for material supplies.*

The DLAN Resources Module is designed to track suppliers and supplies of equipment. Users can view contact persons, location, purchasing information, cost, and quantities for equipment rentals.

3. *Record orders and receipts for equipment and supplies.*

All orders and receipts for equipment and supplies can be tracked within a DLAN Ticket. The Ticket serves as a central place that aggregates all information related to a task, from the initial resource request, through logistics, procurement, resource deployment, demobilization, and finance recovery. Orders and receipts for equipment and supplies can be uploaded to the ticket as an attachment.

4. *Provide capability for the upload/import of database of existing or acquired inventories.*

As part of WV's project implementation, BCG will import a database of existing or acquired inventories into DLAN. This is typically achieved through the upload of an excel or CSV file of data. BCG can provide a recommended import template for resources. After initial implementation, WV's DLAN maintenance and support plan entitles the state to several imports or refreshes per year to maintain the data.

6. *The EMIS must enable users to provide cost analysis services including the ability to:*

1. *Identify material and personnel that require payment.*

The finance tab in a DLAN ticket can be used to track the material, personnel, and required payments associated with a finance cost. The ticket's statuses can be used to track payment progress and can be adjusted as a cost moves through the system. For example, the ticket status may be set to Procurement Needed, Approved, Payment Pending, Paid, Reimbursement Pending, etc. These statuses are configurable by a system administrator.

The DLAN Incident Ledger page also provides data for reimbursement payments including 25% and 75% reimbursement rates and total sums.

2. *Enter and record all cost data.*

The DLAN Finance Module provides the necessary tools to help users and administrators track costs for missions, tasks, and resources. It is based on FEMA's reporting standards and can also be configured to the state's needs. Finance records can be entered either from the finance tab in a ticket or through the Incident Ledger page. Each finance item is associated with a particular incident and with a ticket that tracks the finance request and its current status. DLAN comes pre-loaded with a resource list and cost codes that are based upon FEMA's equipment list costs. Custom resource codes and costs can also be added by an administrator. Information about the item, delivery info, wage info, and invoicing are all recorded by the system.

3. *Maintain accurate records of incident costs.*

The DLAN Finance Module's Incident Ledger feature allows users to quickly generate custom reports about financial items for the current incident. All finance pages support searchable and sortable data columns, exporting data to Excel, Word, or CSV files, and automatic subtotaling and totaling sums. This means that the current spend level for the incident is always totaled and available.

4. *Support planning activities through preparation of estimates for resource usage.*

DLAN supports planning activities including the preparation of estimates and expected resource usage through the use of the Preparedness Toolkit features. This functionality allows an authorized user or administrator to prepare templated tickets ahead of time for common resource requests and standard mutual aid requests such as mission ready packages. These templated tickets can include all finance information and costs relevant to equipment and personnel involved with the task or mission. Templated tickets can be activated individually or in bulk (mass activated) by an administrator as needed. Templates can also be used by basic users as a way to enter a standardized ticket with pre-filled information in a quick and accurate manner rather than building a resource request ticket from scratch. Finally, templated tickets are associated with a scenario / incident category and can be automatically activated when an incident of that type is created. This provides an immediate action plan and important tasks at the beginning of an incident response when time is most critical.

4.2.1.1.14 *Forms and templates. The EMIS shall provide the electronic fillable and printable forms for users to prepare, share, present, electronically sign, and print required documents.*

DLAN allows administrators or authorized users to design, build, and deploy custom fillable forms such as a contingency operations plan. Forms can include fields, tables, drop-down lists, text, images, and other attributes as well as electronic signature capture fields. DLAN can also track dates and times for a form field, for example automatically record when a form is signed. This can be used to trigger workflows or build in automation. All forms

created in DLAN can be deployed to the Mobile App for users in the field or at other locations to fill out forms and sync the data back to the DLAN system where it can be displayed on a report or dashboard and then managed accordingly as either a ticket or an assessment.

1. The EMIS shall enable electronic and customizable forms.

DLAN provides electronic forms that can be created, customized, and updated by authorized users. Once created, the forms can be used with the resource request process, assessment process, role checklist process, the GIS map, ArcGIS, reporting, templates, the mobile app, and more.

2. The EMIS shall allow users to update, create or import user generated forms. System upgrades must allow for continued use of previously generated forms.

Users in DLAN have the ability to create custom forms within the system using a simple no-code WYSIWYG style form builder tool. Existing web forms can be imported into the system by copying and pasting the html of the form into the DLAN EMIS form builder tool. Forms in other formats such as a MS Word document can be saved as a web page and then opened with notepad to copy and paste the contents into the EMIS to import the form.

System upgrades do not affect the ability to use previously generated forms. Updating a form layout with new fields or information will not impact historical records with the old version of the form, only newly created entries going forward. Or, administrators can choose to override and update old instances of the form to the new version.

4.2.1.1.15 Situational Awareness. The EMIS shall be able to provide tailored views.

Customized views can be created out of any of the modules and situational awareness panels on the system to allow for user, role, and task specific views to be created and re-used. These dashboards can also be set as a user's or role's landing page (homepage) in the DLAN system. Combined with Workflow Mappings, this presents a completely tailored user experience for each federal or state agency, local jurisdiction, NGO or any other organizations on the system.

1. The EMIS's situation display shall be able to display geographical views with geo-referenced features on map overlays.

DLAN's GIS Premium module provides geographical views of selected areas and allows users to activate map layers that appear in real time with accurate geo-referenced data.

2. The EMIS's situation display shall be capable of displaying one or more selectable map overlays.

Map Reports can be used to display specific map information. GIS administrators can configure map reports including basemap and layer settings to be viewed in the GIS display or as part of a status board. They can also display multiple map overlays and seamlessly integrate said layers into the map in real time.

DLAN's GIS Premium module allows for multiple map overlays to be activated at once and shown on the Legend column.

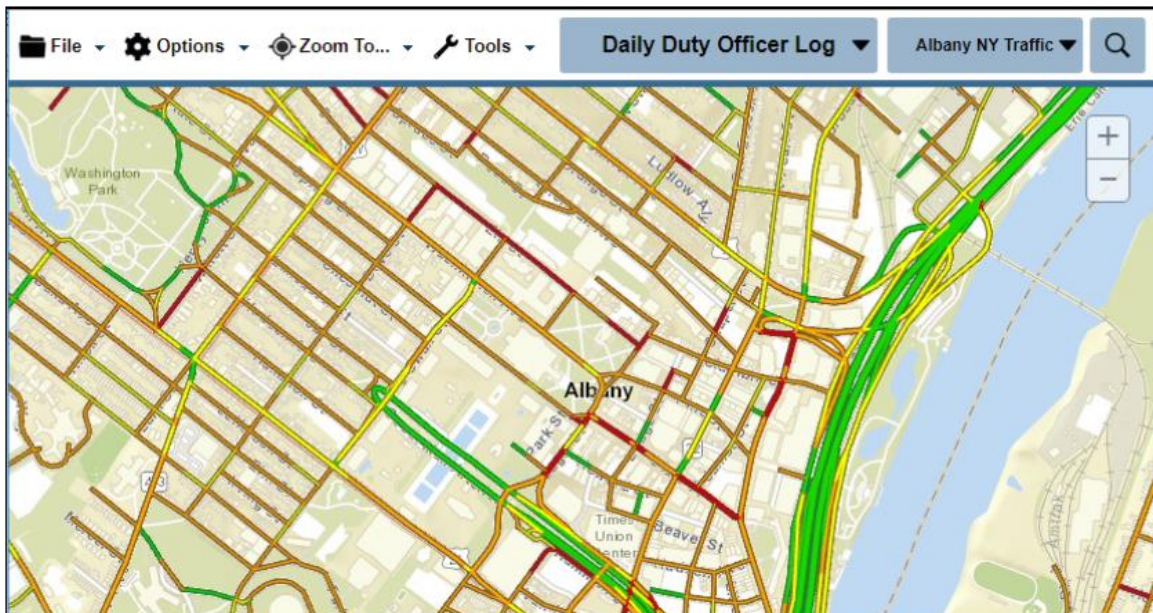


Figure 16: Map Report - Traffic

3. *The EMIS's situation display shall be capable of displaying a situation report, operational information, status report, or map image received from users.*

DLAN's Status Boards can display any information from within DLAN and from multiple external sources, including situation reports, operational information, status reports, or map images received from users.

4. *The EMIS's situation display shall include the ability to display selectable levels of detail to enable users to see summaries such as a dashboard display to indicate elements that may require attention.*

The DLAN Status Boards (dashboards) allow both overview and macro views of incident status information and detailed status information on roles, teams, tasks, and critical incident messages. Status Boards update automatically in real-time as new information is entered.

Several tools are available on the Status Board to help users drill down to key status information including the Stats page which shows statistics based on role and task; Ticket Reports, which show individual tasks and their completeness; and incident messages, which allow users to post situational awareness information or critical decisions.

5. *The EMIS's situation display shall be capable of integrating and displaying live images and audio/video feeds from external sources such as traffic monitors, security cameras, surveillance cameras or data feeds.*

Streaming Video allows you to access any IP-based video feed, including streaming and snapshot cameras, for improved situational awareness. Video streams can be chosen using an easy drop-down menu and displayed simultaneously on the Streaming Video dashboard or be popped out into their own windows

for enhanced viewing. Live images and audio/video feeds can also be displayed directly on the GIS Premium map.

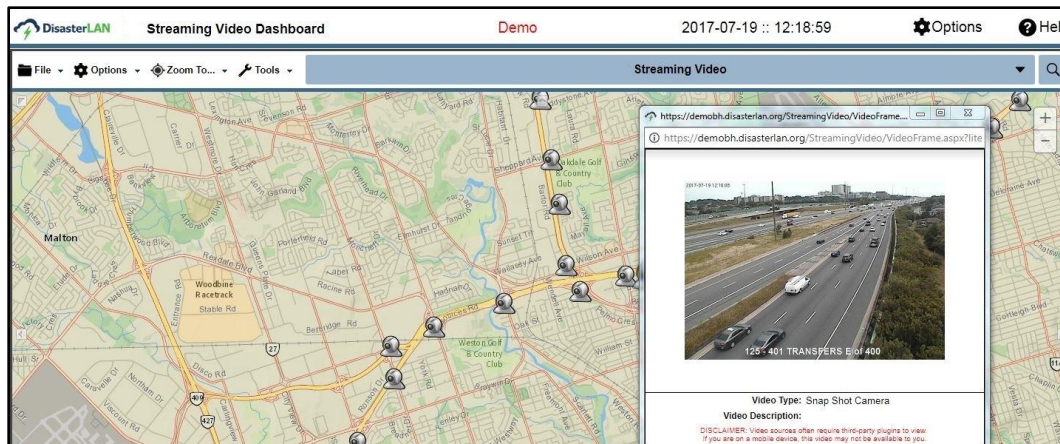


Figure 17: Streaming Video on Map

6. *The EMIS shall be capable of capturing and disseminating the image showing on the situation display to selected user(s).*

Images can be shared within the system to selected users by controlling who has access to a board or image file. Images from the situation display can also be shared internally or externally via message or email.

7. *The EMIS shall provide for managing and reporting of injuries and deaths.*

The system can provide a way to report on injuries and deaths and manage that information through the use of secure tickets. A secure ticket is locked so that the sensitive information contained inside is only visible to roles that have been specifically routed the ticket (shared with them). Secure tickets can be collated in a Ticket Report designed to capture and display that information on a Status Board. Both the report and the board can also be secured so that only specific users get access to them.

4.2.1.1.16 *Community Lifelines. The EMIS shall automatically generate a dashboard, and status based on the Community Lifelines. The EMIS shall allow users to generate and store time-stamped Community Lifelines reports based on jurisdiction and event.*

The DLAN system includes a Community Lifelines toolkit designed to assist users with managing lifeline information and reports. Status Board (dashboard). The toolkit consists of a Community Lifelines data collection form that can be filled out from either the web interface or from the mobile app. The data submitted on the form automatically populates a Community Lifelines Report that displays detailed and critical information. The report is then displayed in a dynamic GIS Map and Dashboard with color coding for condition and trend on each event as well as other critical information. This overall workflow allows users to create lifeline reports for all of FEMA's seven community lifelines (Safety and Security; Health and Medical; Communications; Hazardous Materials; Food, Water, Shelter; Energy (Power & Fuel); and Transportation.). The result is time stamped and accurate reports that are filterable by lifeline, jurisdiction, and event kind that provide a way to make better informed emergency decisions.

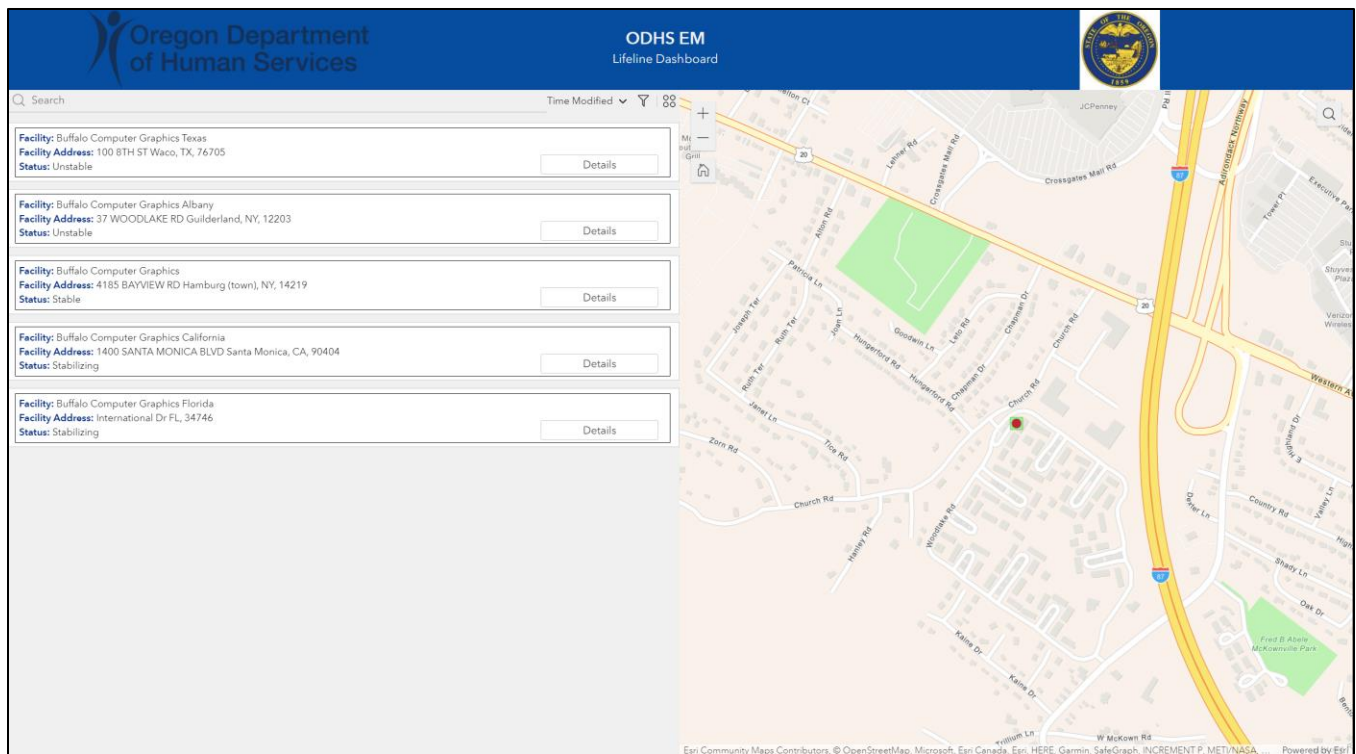


Figure 18: Community Lifelines Dashboard

4.2.1.1.17 *Communication. The EMIS shall offer chat rooms and virtual conference rooms configurable by users. The EMIS shall enable the users to capture and manage content. The EMIS shall enable the users to save and store documents, recordings, and aids used in a chat room or virtual meeting.*

The Chat Module is DLAN’s internal instant messaging system and is included with all systems. It can be used to send and receive user-to-user messages. When sending a chat, the system will display other users that are online as well as their role (function) to make finding the correct person simple. All chat history is saved and can be viewed by the participants as well as by an administrator with advanced permissions. This means that any documents, recordings, or aids will be saved and accessible. Users can also initiate chat rooms for multiple participants. Chat rooms can be initiated independently or from within a ticket and saved as part of the ticket log, eliminating the need for duplicate data entry and creating a more complete record of decisions.

1. *The EMIS must provide the means to communicate easily with one or more remote users (by name or by function) using real time text messaging that is logged and recorded.*

Using the Chat Module, DLAN allows users to send messages to other users on a one-on-one basis or in a group in real time. All chat history is saved and can be viewed by participants as well as by an administrator with advanced permissions.

2. *The EMIS must have the ability to send automated text messages, voice chat messages, or video messages to mobile devices.*

DLAN can send automated or manually triggered text messages, voice phone calls, and emails to landlines, mobile phones, and users' devices. This includes voice only capable devices. DLAN provides automated text and email messaging when an incident is created, when a situation report is due, and when a user is offline but a ticket has been routed to his or her role. Any messages sent to the device that is voice only capable will be handled by the device's native operating system.

3. The EMIS shall be capable of logging chat history in order to be retrieved by users at a later time.

All chat history is saved and can be viewed by participants afterwards in the Communication Center module. Chat history can also be accessed by an administrator with advanced permissions for audit or review purposes.

4.2.1.2 Software Administration. The EMIS's administrative and management functions shall be available to the system administrators.

System administrators have access to a large number of administrative and management functions within the DLAN software and the system is fully self-administrable by the client. A Full System Administration suite allows your administrators the ability to update and adapt the settings, preferences, lists, and values in real time as well as build their own dashboards and forms without needing vendor support and at no additional cost. Administration is available through the UI using simple tools, so no additional staff is needed to code or manage the system. This provides lower total cost of ownership over time.

With DLAN there is no need to use separate administrative menus for different areas of the system; universal system changes can be made from one easy to use menu. The System Administration menu includes three main categories: modules, system setup, and site security.

- Standard System Administration includes:
 - Site Security info: User, Group, and Role Management- The Site Security page can be used by administrators to create and manage user accounts, user/record level security groups, roles, and navigation menu links. Together these features allow the system to be customized to match a customer's workflow at no additional cost.
 - Module Administration settings- DLAN provides module administration pages can be used by administrators to change the configuration options for individual modules.
 - System Settings- The System Setup page can be used by administrators for configuration, presentation, and security settings that affect global DLAN system, not an individual module. For example, password security strength settings, login page graphics and text, and prohibited file type uploads.

4.2.1.2.1 The EMIS must provide user access through desktops, laptops, and mobile devices, such as, tablets or smart phones. The EMIS must let a user remain logged in at the same time on different devices.

DLAN is accessible through any web browser and also has a mobile app that works with Apple and Android phones and tablets. Additionally, a Windows app is available for use on desktops or laptops in addition to

accessing the site through the web-browser. A user can log into their account at the same time from both the web and on the mobile app.

4.2.1.2.2 *The EMIS must enable a user to sign on 'once' for access to all embedded applications.*

Single Sign-On can be implemented in DLAN. DLAN integrates with existing systems and includes single sign-on options for ease of use for users. The DLAN system tools allows for basic LDAP and Active Directory integration. It also includes tools for multi-factor authentication (MFA). Once a user is signed in they have access to all embedded applications.

Support for multiple simultaneous federated authentication / single-sign-on sources (as well as a hybrid model that supports both federated accounts for core users, and local user accounts for outside stakeholders and other agencies) DLAN supports federated authentication through Active Directory Federated Services accounts, SAML based accounts, and Active Directory (LDAP) based accounts. Any mix of these types of accounts can be utilized on the system at the same time.

DLAN's Single Sign On tools allow for Active Directory/SAML 2.0 based accounts to easily be utilized to setup default permissions, roles, access to content, access to data, and other settings within a user's account. The system also supports the use of multiple federations simultaneously so that a regional solution will support multiple organizations, each with its own active directory integration for provisioning and authenticating user accounts.

The following are available for Security Integrations:

- LDAP (outbound authentication)
- LDAP pre-registration (inbound user list synchronization)
- Federated Services (SAML 2.0, Shibboleth via ADFS)
- API based Integrations with Third Parties:
- Ticket Data API (two-way data sharing)
- EDXL-DE API (two-way data sharing)
- EDXL-CAP API (two-way data sharing)
- EDXL-HAVE API (inbound data sharing)
- EDXL-RM API (inbound data sharing)
- CAP API (two-way data sharing)

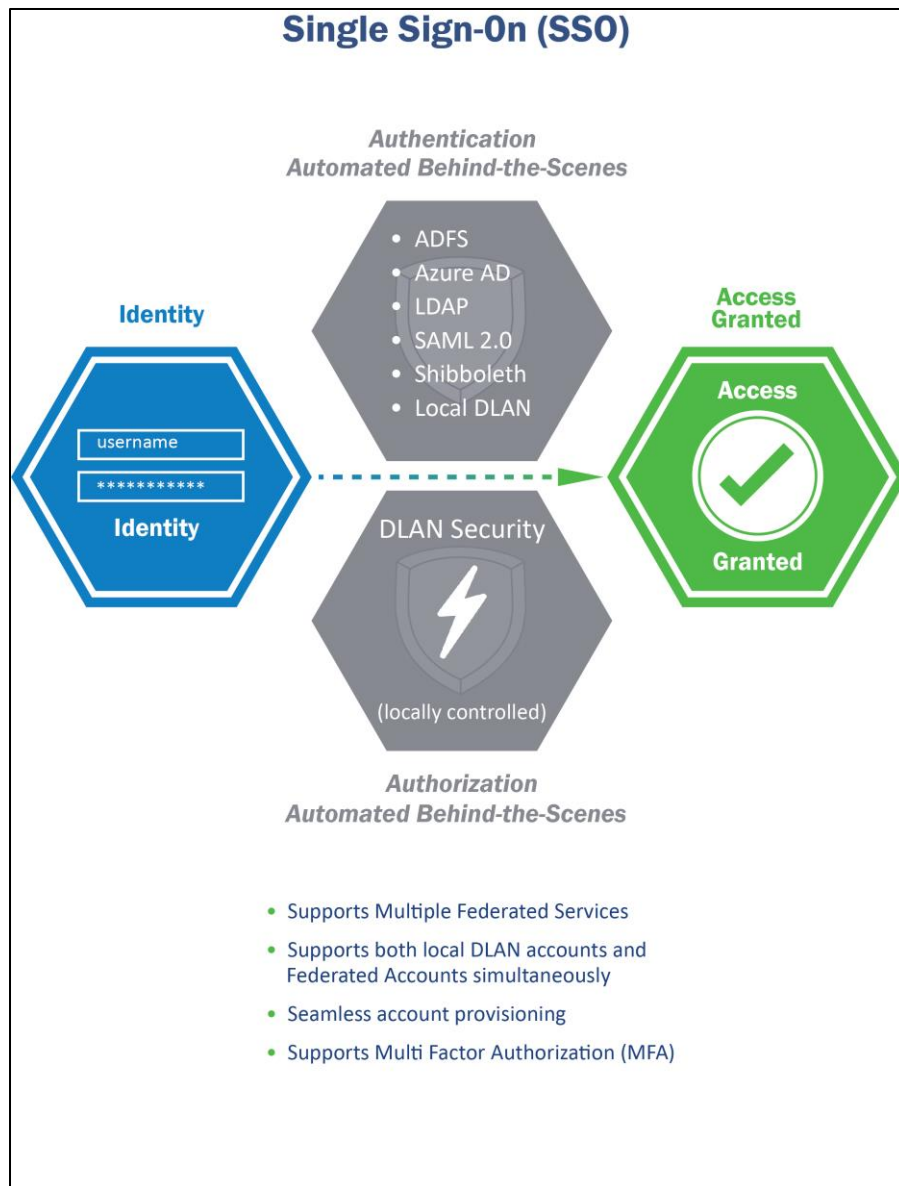


Figure 19: Single Sign On

4.2.1.2.3 *The EMIS shall be able to define a structured top-level organization with fully functional sub-organizations that operate in a hierarchy of authority.*

DLAN provides a structured top-level organization and fully functional sub-organizations through the use of its Record-Level data groups. These can be built-out as needed by a State System administrator. Users, permissions, and security can be assigned to the group.

4.2.1.3 Technical Requirements

4.2.1.3.1 *The EMIS shall be compatible with multiple factor identification and its use for system access.*

DLAN does not currently support multiple factor identification. This can be added as a customization; not included in proposal pricing.

4.2.1.3.2 The EMIS shall provide for single sign on and for PIV/PIV- 1/CAC integration for system access based on Federal Information Processing Standard (FIPS 201-2) requirements.

<https://csrc.nist.gov/publications/detail/fips/201/2/final>

DLAN does not currently support single sign on through PIV/PIV-1/CAC. This can be added as a customization; not included in proposal pricing.

4.2.1.3.3 The EMIS shall record the failure of a login attempt. The solution shall have the flexibility to lock the user account after an Administrator-specified number of attempts. The solution shall have the capability of providing unattended password reset capability.

DLAN includes a security violations report that shows failed login attempts.

Username	Time	Resource	IP Address	Description
bog_cfne	3/19/2019 11:38:40 AM	jscoop.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /gis/jscoop.aspx?IsStatusboardMode=true&mapReportid=60 UserID (untrusted)= 1289 SessionUserId (untrusted) = 9881
bog_cfne	3/19/2019 11:38:39 AM	JSCOP.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /GIS/JSCOP.aspx UserID (untrusted)= 1289 SessionUserId (untrusted) = 9881
bog_cfne	3/19/2019 11:38:29 AM	SiteSecurity.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /Admin/Security/SiteSecurity.aspx UserID (untrusted)= 1289 SessionUserId (untrusted) = 9880
mward	3/19/2019 9:10:10 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
mward	3/19/2019 9:10:09 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
mward	3/19/2019 9:09:58 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
bog_msaleh	1/8/2019 10:22:08 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
bog_msaleh	1/8/2019 10:22:08 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
cfne	10/30/2018 9:48:36 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
cfne	10/30/2018 9:48:35 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination

Figure 20: System Administration - Security Violation Report

Administrators can specify the number of attempts before a user will be locked out in the Security Settings. The system also allows users to reset their password using a question and response method.

System Administration: Security Settings

Save Cancel

Enforce Strong Passwords: On Off

Passwords must be at least characters long

Passwords must contain at least lowercase character(s)

Passwords must contain at least UPPERCASE character(s)

Passwords must contain at least numeric character(s)

Passwords must contain at least special character(s)

Password Reuse

Users can reuse passwords

Prevent users from reusing the last passwords

Prevent users from reusing passwords

Bad Password User Locking: On Off

If user fails password attempts within minute(s), lock account for minute(s)

Require Phone on Login: Yes No

Require Role Selection on Login: Yes No

Allow Account Recovery: Yes No

Session Timeout in Minutes:

User Inactivity Logout Time (Minutes):

Duration to wait for answer (Seconds):

Mobile Responder App Timeout Window (Minutes):

Figure 21: System Administration - Security Settings

4.2.1.3.4 *The EMIS shall have the ability to provide event logging for successful logins, IP addresses of every authenticated user, failed login attempts, IP addresses of every failed login attempt, user database changes, log failures and/or errors.*

All of these report types listed here are available within DLAN’s System Administration.

4.2.1.3.5 *The EMIS shall include the means of recovering from a system failure using data previously backed-up.*

DLAN provides automatic recovery of data in several ways. First, all DLAN tickets have an auto-save feature that backs up a copy of the information the user has entered to their browser’s local cache. This means that if the user accidentally closes the ticket without saving, or loses connectivity, they can recover their draft to continue working.

At the technical level, DLAN services are resilient and will automatically self-restart if a service goes down or becomes unavailable. DLAN also supports load balanced servers, automatic or manual failover to another node, and a disaster recovery site.

4.2.1.3.6 *The EMIS shall limit access to those users who have valid login permissions and credentials.*

All users must have valid login permissions and credentials to access DLAN.

4.2.1.3.7 *The EMIS log in procedure shall include a requirement for users to agree to the state's confidentiality agreement prior to gaining access on each log in.*

DLAN includes a customizable User Agreement that be setup so each user has to click accept each time they log in. This agreement can either include the full text of the state’s confidentiality agreement or link to it, depending on the State’s preference.

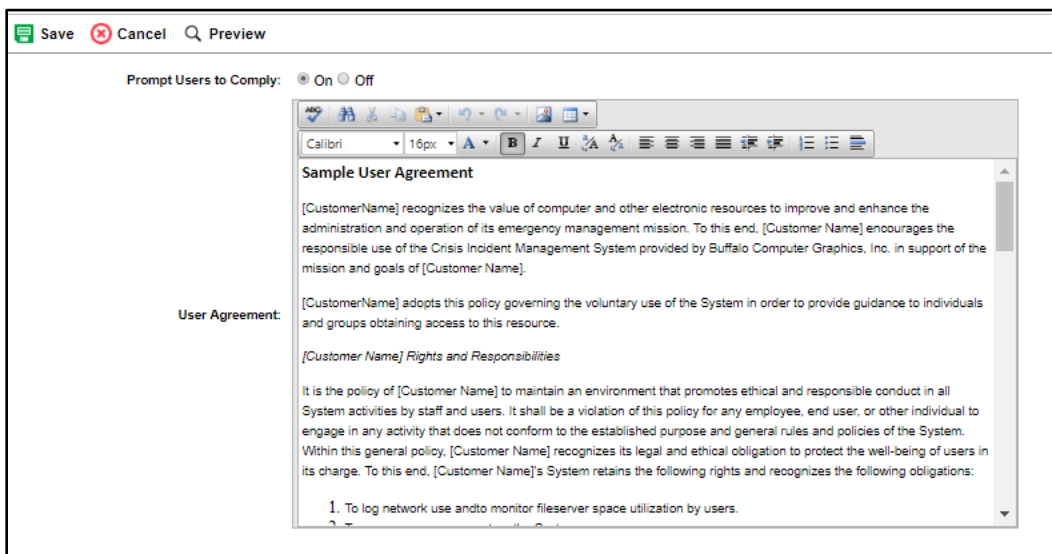


Figure 22: System Administration - User Agreement

4.2.1.3.8 The EMIS shall enforce strong alphanumeric passwords and periodic password changes. It means, minimum eight characters, combination of numbers, letters, special characters, and monthly password changes.

DLAN includes customizable password settings, please see Figure 21: System Administration - Security Settings on page 68.

4.2.1.3.9 The EMIS shall provide capability of a user to obtain password reset by administrator and by verification and via approved email and/or text.

Administrators can reset passwords either in bulk or individually. When a user's password is reset they are sent an email notification.

4.2.1.3.10 The EMIS shall be scalable to automatically accept any number of users to a maximum of 500 users logged in simultaneously with capability to add additional users with no delay.

The DLAN EMIS is scalable and can easily support up to 500 concurrent users logged into the system simultaneously. Additional users can be added on the fly and are not prohibited from accessing the system. Cloud hosting resources will be assigned to support the 500 user load and can be increased on demand by authorizing BCG support to do so. Please Figure 23: Scalability below for additional information.

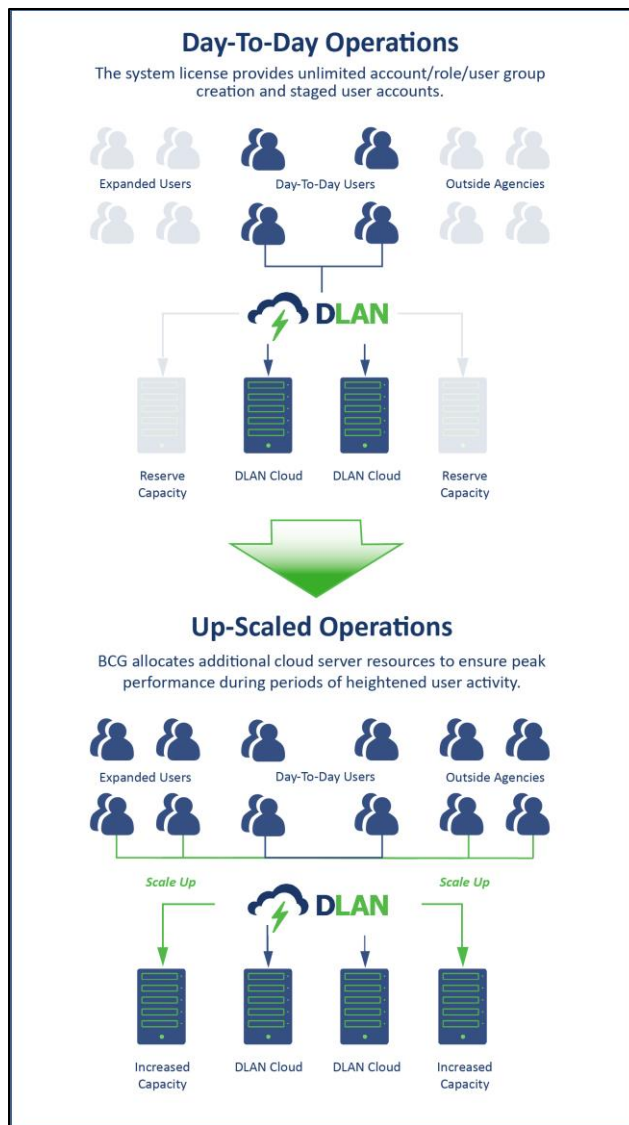


Figure 23: Scalability

4.2.1.3.11 The EMIS shall adhere to industry standard scalable relational database architectures that are able to provide input or output to other Enterprise systems.

DLAN’s database runs on Microsoft SQL Server version 2012 or later (newer versions preferred). Any standard method of data exchange supported by SQL should be available to use with the DLAN software system.

4.2.1.3.12 The EMIS’s Graphical User Interface (GUI) shall be a windows-based interface, and mobile app User Interfaces (UI).

DLAN is a web-based software system that runs on MS SQL and IIS and can be accessed from any computer, laptop, or device that supports a modern web browser (IE 11, Edge, Chrome, Firefox, or Safari) as well as browsers on mobile device such as chrome, android, and safari for iOS. DLAN is useable on both Windows and Mac systems. The DLAN Mobile Responder App is available for iOS, Android, and as a Windows App.

4.2.1.3.13 The EMIS shall have three environments: production, training, and development environments. The training and development platform shall have the same functionality and capabilities of the production platform. The development platform will be used for change management. The training platform will be used for training, exercises, and scenario modeling.

BCG will provide a development, training, and production environment. These platforms are separate so that the data will stay separated. The same features and functionality are available on all environments.

4.2.1.3.14 The EMIS shall have complete redundancy across all components and a sole Disaster Recovery solution, in the event of data corruption, hardware malfunction, or cyber- attacks.

DLAN supports multi-node configurations, virtualization, high availability, load balancing, and disaster recovery. DLAN is also a secure solution and follows guidelines for NIST 800-53 and NEIM. DLAN receives regular security and penetration testing by multiple customers per year. All tests are run by reputable third parties and BCG works with customers to address any potential threats.

For this solution BCG will provide a sole Disaster Recovery solution that will safeguard data and allow the system to be returned to operation in case of impact the primary and secondary replication sites.

4.2.1.3.15 The EMIS shall have multi-server fault-tolerant architecture with full redundancy and automatic recovery.

DLAN uses a multi-server fault-tolerant architecture. It can support redundancy through active/active or active/passive servers for load balancing, failover, and recovery.

BCG asked several clarification questions during the Q&A period as well as asking for clarification on the answers provided by VWDEM after addendum #2 was issued. BCG is providing the following attributes based on our best understanding of the desired system architecture as described in the RFP and Addendums. However this approach can be adjusted prior to contract award if needed. Please see Figure 24: Cloud Hosting Specifications below.



Figure 24: Cloud Hosting Specifications

- BCG will provide adequate burstable bandwidth to support system performance for VWDEM.
- BCG will use VPN over the public internet for transfer, or simple TLS 1.2 encryption for transport.
- BCG will provide adequate file share storage (up to 1 Terabyte).
- BCG assumes 99.9% guaranteed uptime for system availability not including planned updates. Realized annual uptime on BCG systems is often closer to 99.99%.
- Disaster recovery or failover between sites may require some brief manual intervention by BCG's 24x7x365 support engineers. Disaster recovery or failover may incur additional costs or services that are not covered in the basic monthly charges and will be provided at a time and materials basis by BCG pending WVDEM's approval.

4.2.1.3.16 *The EMIS shall support multi-site architecture that provides for the following replication sites and supports an Active/Active platform for high- availability and load balancing. The sites must meet the following minimums.*

1. *Primary replication site at least 50 miles from our facility.*

BCG shall provide an Active/Active platform for hosting of the EMIS application using Amazon Web Services with availability zones for redundancy and high availability. BCG shall provide load balancers to direct traffic

to the appropriate server. The hosting shall support up to 500 concurrent users with the capacity to surge user connections in excess of that number if needed.

BCG will provide the Primary replication site in AWS' Virginia location which will meet the requirement for it to be at least 50 miles from WVDEM's facility.

2. Secondary replication site at least 100 miles from our facility and at least 100 miles from the primary replication.

BCG will provide a secondary replication site located on in Ohio, which will meet the requirement that the site be at least 100 miles from WVDEM's facility and the Primary site.

3. Tertiary replication site at least 200 miles from our facility. and at least 200 miles from the secondary replication.

BCG will provide a tertiary replication site in California, which will meet the requirement that the site be at least 200 miles from WVDEM's facility and the Primary site.

BCG will provide a target Recovery Time Objective (RTO) of 72 hours and a target Recovery Point Objective (RPO) of 24 hours.

The vendor shall provide a copy of their disaster recovery plan upon Agency request.

BCG agrees to provide a copy of our disaster recovery plan upon Agency request.

4.2.1.3.17 The EMIS shall provide data backup to include error checking and correcting during backup to ensure backed-up data is valid.

DLAN supports backups through any software or platform that supports operation on MS SQL server databases. This includes the ability to error check and correct data during a backup to ensure data is valid. BCG is proposing an on-premise installation for this project so the state would be able to implement a backup solution of their choice. Data replicated to the primary, secondary, and tertiary replication sites can also be backed up.

4.2.1.3.18 The EMIS shall provide for records maintenance and retain information until permanently deleted.

DLAN logs and maintains all records within the system. Typically, deleted data is "soft deleted" meaning that it is hidden from display to the user, not removed from the database. Typically, there is no reason to permanently delete record data within DLAN as data can be archived or soft deleted when no longer needed.

4.2.1.3.19 The EMIS shall provide flexible emergency management support functions for day-to-day operations and large-scale multi-agency response.

DLAN is specifically designed to support daily operations and emergency responses. Integrating Incident Management Software into daily operations is the gold standard for getting staff familiar with the software and prepared to utilize it during an emergency. BCG highly recommends customers find ways to utilize the software in daily operations and provides several tools that can be used on a daily basis for normal operations, including

event logging, social media monitoring, email monitoring, webpage/RSS feed monitoring, documentation library folders, role-based briefing notes, and several other tracking tools.

In addition to these daily use monitoring and documentation tools DLAN provides a common platform for task, resource, and information management system that can be applied to various types of needs and workflows. Documentation management and sharing is another area that sees regular system usage within daily operations through the use of our Reference Library. DLAN can be used to monitor incoming information and easily move from event monitoring to emergency activation.

DLAN is designed to work across multiple agencies with features such as location and group based access, user and role based boards, multi-tiered security settings, and incident locking. The permissions structure in DLAN can be configured by the customer to have granular security permission, broad security permissions, or any range in between. Using these same security permissions whole incidents can be locked down to only specific facilities. In this way DLAN balances the need for collaboration and the need for privacy among multiple agencies and stakeholders. Additionally, DLAN provides for the development of contact lists and personnel databases to support communication across multiple agencies and the custom development of standard operating procedures and checklists to facilitate a unified response.

4.2.1.3.20 The EMIS emergency management support functions shall enable users to share, analyze, and prioritize information across multiple jurisdictions in text, images, and geo-referenced map formats.

DLAN allows information to be shared across multiple jurisdictions in numerous formats including text, images, and geo-referenced map formats. With DLAN users from different jurisdictions and agencies can work together on a common unified platform to share, analyze, and prioritize information for an improved response effort. Text, images, and maps can be posted to a Status Board (dashboard) to share them with other jurisdictions. This information can also be shared within other modules and system features such as tickets, messages, emails, file storage libraries, and GIS map reports.

4.2.1.3.21 The EMIS shall operate as a web application in which users interact with the EMIS through any web browser, and mobile applications.

DLAN is a web-based solution that is able to work across multiple OS platforms, browsers, and mobile devices. Please see Figure 25: Browser and Device below.

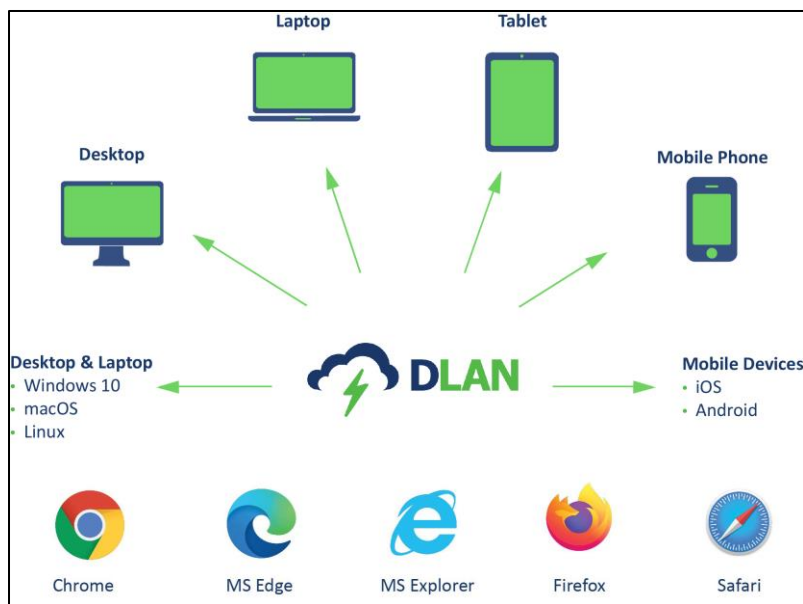


Figure 25: Browser and Device Compatibility

DLAN testers and engineers test DLAN modules and tools on several browsers to ensure that the platform can be used on the greatest number of browsers as possible. This includes testing the product on Internet Explorer 11, Edge, Firefox, Safari, Safari on iOS, Chrome, Chrome on Android, and Android browsers.

In general, DLAN is designed to be accessible from any mobile browser that fully supports JavaScript, session-based cookies, HTML 5 technologies, and other modern web browser features. DLAN’s responsive design interface allows many mobile devices to support DLAN natively (i.e. no app required) including Apple iOS Devices, Windows Mobile Devices, and Android Devices.

Since modern browsers are regularly updated, BCG developers are constantly reviewing and retesting on all major browser platforms so that they can identify changes or issues and adapt the system to work on the widest range of browser platforms as possible. An agile development process and regular product updates (typically every 8-10 weeks) allows DLAN to remain web and mobile browser agnostic.

4.2.1.3.22 *The EMIS shall be browser independent, and device awareness industry requirements.*

The DLAN EMIS is browser independent, supporting the latest versions of Chrome, Edge, Firefox, and Safari on desktop, and Chrome and Safari on mobile devices. DLAN is accessible from any modern mobile devices through the device’s web browser. Additionally, a native mobile application is available for iOS and Android devices.

4.2.1.3.23 *The EMIS shall be built on a highly secure platform. The Vendor shall describe their platform and security measures such as end-to-end encryption.*

DLAN is fully compliant with the AES256 standard. Passwords and other sensitive information are encrypted in the database using AES with 256 bit keys. In addition, all encrypted data is indexed with a hashed lookup code so it is impossible to determine what the data context is without previous knowledge of the key used to store the information. During transmission DLAN relies on HTTPS using TLS for client to server communications. For Internet mail capabilities transmission can occur in plain text, SSL, or TLS.

DLAN passes a biannual security audit conducted by a State Level Department of Homeland Security and Emergency Services who utilize DLAN for their operations. This scan looks for vulnerabilities in IIS, .Net, SQL, and other components of all forward facing websites deployed. DLAN has also passed independent security audits for multiple customers on all system components. Third party system reviews were conducted by established and reputable audit firms such as C2 and Deloitte. BCG is also a member of the Federal Bureau of Investigation’s Infragard team dedicated to identifying and neutralizing threats to critical infrastructure and software and has a full-time CISSP employed on staff.

4.2.1.3.24 *The EMIS shall provide secure usage capabilities such as security reporting, user data access, and email/message.*

The DLAN EMIS is a secure system. The System Administration pages provide authorized users and administrators access to standard reports, user information, message queue data, and monitoring capabilities:

Admin: Site Security	
Users	Groups
Roles	Modules
Reports	
Report Name	
Currently Locked Out Users	
Currently Logged in Users	
Group Modules	
Mobile Responder Users	
Module Users	
Routing Permissions - Who a Role Can Route to	
Routing Permissions - Who Can Route to a Role	
Security Violations	
User Activity	
User Agreement Compliance	
User Groups / Incidents	
User Groups / Modules	
User Groups / Modules / Items	
User Login History	
User Login Timeline	
Users Last Changed PWs	
Watch Command Activity	

Figure 26: Administrator and Usage Reports

In addition to the standard reports shown in Figure 26: Administrator and Usage Reports, the system also provides a message queue page that lists all email/messaging records, their status, and other key information.

4.2.1.3.25 *The EMIS shall enforce secure networking protocols and ports for all activities.*

DLAN adheres to and utilizes multiple ratified and draft RFC standards in its implementation. These include, but are not limited to:

- SMTP (5321, 6152)
- MIME (2045, 2046)
- POP3 (1939)
- IMAP (3501)
- TCP (793)
- IP (791)
- UDP (768)
- RPC (5531)
- TIFF (3302)
- HTTP (2616, 2617)

4.2.1.3.26 The EMIS shall maintain an event log of all entries, which makes a time-stamped record of receipt and transmission of messages.

All information added or modified in DLAN is automatically date and time stamped and displayed in the user interface. All messages and entries are logged along with a record of receipt and pertinent information. Event logs are available both during and after an incident, and historically can be accessed by administrators for view at any time. They are helpful for creating after action reports.

Additionally, history tracking reports are available from a number of different modules in DLAN. The event log history is available for all log entries and shows who created, viewed, or edited the item. An event history by user is available using the Role Activity Log report. When an event or incident is completed it can be deactivated/archived. Archiving an incident makes it unavailable to general users, but administrators or designated users can access it for reporting and analysis or reactivate it as needed. All previous incident responses and their event/ticket log history are archived in the system for easy after action reporting or for auditing purposes.

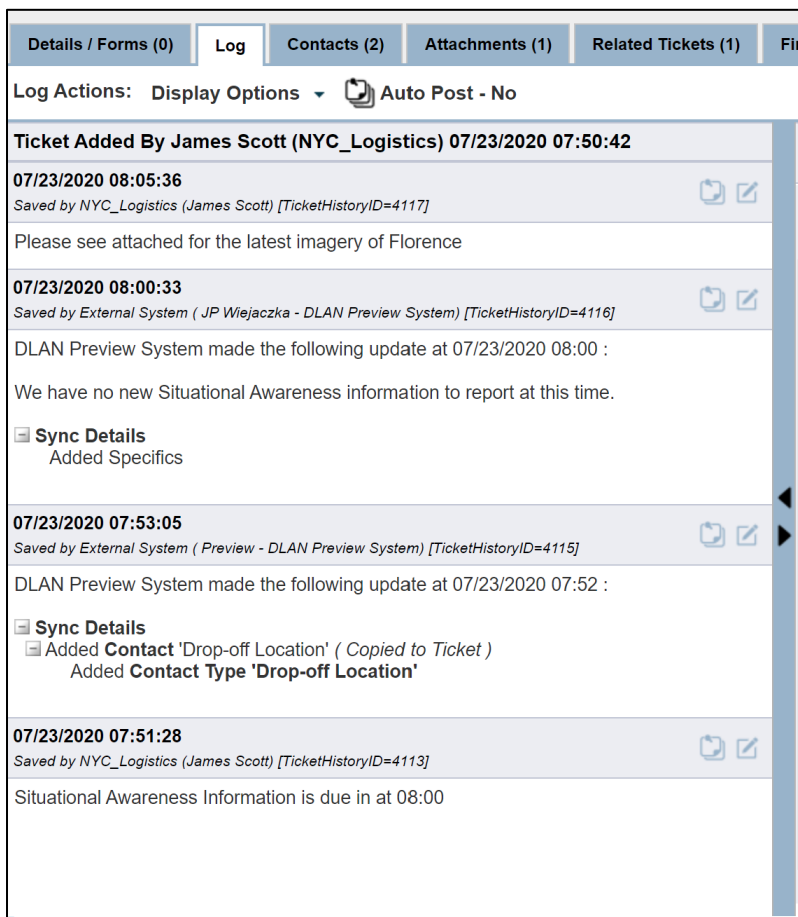


Figure 27: Event Log

Another example is the Status Board History Tracking Report. The Status Board Module tracks all changes made to each board. From the print board screen history tracking can be turned on and a date range can be selected to produce a history tracking report.

4.2.1.3.27 The EMIS shall create and maintain a security audit trail to log system usage.

DLAN is a fully audit ready system with full incident reporting and history tracking to support audit trail capabilities. The Incident Report feature provides a full chronological log of all system usage. The report can be run at the end of an incident before it is archived, or it can be run as a spot report at any point while the incident is active.

All information within the system is logged and time-stamped as illustrated by the Incident Report below.

Incident Report: Summer Storm

Downloads: [Incident Action Plans](#) [ICS Forms](#) [Situation Reports](#) [Incident Folders](#) [COP Screen Shots](#)

Start Date: 11/1/2017 End Date: 12/14/2017

Type: Tickets; DMail Messages; Statu Order Items: Chronologically Run Report

1 of 1 | Export to the selected format | Export

Incident Report as of 12/14/2017 11:08:53 AM For Incident: Summer Storm
Includes Items Of Type: Tickets, DMail Messages, Status Boards, Broadcasts, Situation Reports, Form Instances, IAPs, Folders and Resources, COP Screen Shot
Includes Items from 11/1/2017 12:00:00 AM to 12/14/2017 11:08:53 AM
Ordered: Chronologically

11/8/2017 4:15:07 PM - Incident Action Plan Created On: 6/29/2016 2:17:55 PM. Modified by Cerra, Patrick
12/7/2017 3:16:40 PM - Ticket Manager Ticket - 3224 Created On: 6/2/2016 9:57:40 AM. Modified by Cerra, Patrick (Finance & Administration Section Chief) Ticket Modified as follows: Added the following specifics: Incident Command has approved expenses for additional beds and resources to be provided to the Main St. Shelter. Additional details to follow.
12/13/2017 3:28:37 PM - Ticket Manager Ticket - 3295 Created On: 10/17/2016 9:28:29 AM. Modified by Thompson, Ava (Logistics Section Chief) Ticket Modified as follows: Added the following specifics: Team Assigned.
12/13/2017 3:29:11 PM - Ticket Manager Ticket - 3295 Created On: 10/17/2016 9:28:29 AM. Modified by Thompson, Ava (Logistics Section Chief) Ticket Modified as follows: Changed status to Assigned to Location

Printed on: 12/14/2017 11:08:53 AM 1 of 1

Figure 28: Event Log & Incident Report

4.2.1.3.28 The EMIS shall have an automated and scheduled back up of information, including back up of image libraries, recording libraries, and document libraries.

BCG will provide a backup service for the EMIS. Backups include both the database and file storage. Typically, BCG provides 15 minute incremental backups with daily full backups. These can be set to run at a scheduled time such as off-hours in order to reduce any potential impact to performance.

4.2.1.3.29 The EMIS shall support interaction with remote users using a workstation, laptop, tablet, and mobile devices.

DLAN is a web-based application that can be used on a workstation, laptop, tablet, or mobile device. For additional compatibility information, please refer to Figure 25: Browser and Device Compatibility.

4.2.1.3.30 *The EMIS shall be able to access, integrate, interoperate, and remain compatible with the Agency GIS platform (ESRI - ArcGIS).*

BCG has been providing ESRI based GIS Mapping capabilities inside the DLAN EMIS since 2004. The system is integrated with the Agency’s ESRI ArcGIS platform out of the box. All basemaps, geocoders, layers, and services are compatible. ESRI ArcGIS dashboards and experiences are also compatible and can be displayed in a DLAN Status Board. Additionally, DLAN’s integration with ArcGIS functions with both Enterprise/Portal and ArcGIS Online. Data can be synced in real time between the DLAN ticket manager module, assets module, and other system data sets and ArcGIS.

4.2.1.3.31 *The EMIS shall have an alternate GIS platform that can be used if the Agency GIS platform source is unavailable.*

DLAN is fully integrated with ESRI’s ArcGIS Online. Ticket Report data can be synced in real time to ArcGIS Online (AGO) for either public or private viewing and (if permitted) editing on the AGO platform. DLAN’s integration with AGO also supports the ability for users to fill out forms on the AGO map and sync the data back to DLAN. The system also supports Open Geospatial elements and GeoJSON data services if needed.

4.2.1.3.32 *Support and Maintenance of the EMIS for the period of the contract shall include all upgrades or enhancements, bug fixes, document changes, system support including a technical hotline and support services to support the requirements of this system.*

For this project BCG is proposing our **Gold Plus Support package**, which includes everything West Virginia requires. It will provide all upgrades and enhancements, bug fixes, online document changes, system support including a technical hotline and support services to support your staff and the requirements of your system. The Gold Plus Support Package we recommend is defined as follows:

Maintenance & Support Service Provided *	Gold	Plus
Business Day (9am – 5pm PST) Email and Phone Support	✓	Plus can be added to any support package
24/7 Emergency Activation Phone Support	4 cases per year	
BCG Assisted Patching Support	24/7	
New Releases of Product	✓	
New Release Review Webinars	✓	
Hot Fixes for New Releases	✓	
Point Patches for New Releases	✓	
Rush Delivery of Hot Fixes Specific to Organization’s Site or Installation		
Server Node Support	Up to 2 Nodes	
Custom BCG Services	40 hours per year	

Onsite Support		
Unlimited 24/7 Support		✓

*Terms and Conditions Apply

4.2.1.3.33 The Vendor shall provide a proposed EMIS support model. The proposed support model must identify how the vendor will address the ongoing support functions.

BCG believes that the high level of support we provide to our customers sets us apart from our competition. We constantly elicit customer feedback and incorporate it into making DLAN a better product. Customer input is always important in the decisions that are made to provide new feature enhancements. If the BCG team feels that a requested customization will be beneficial to other customers, it may be developed at a significantly reduced cost or at no cost and then provided to all customers with a current maintenance & support package.

Help Desk (24x7x365 for WVDEM)

All reported issues will be addressed by the BCG Client Services team. Customer service is a key component to any solution. BCG understands some customers prefer self-service features over working with customer service. BCG also understands a solid help desk is essential to providing top tier support. BCG’s best in class support model and software utilize both methods to provide ease-of-mind as well as ease-of-use.

The BCG Software System includes an online help section that allows users to reference help articles for all pages in the system. Users will also have access to the training materials and quick reference guide developed by the BCG Team for this project.

In addition to this self-service help, the BCG Team will provide a business day customer support help desk that is available to the State. The help desk includes a ticketing system, phone, and email support as needed. BCG also provides an escalation process that helps us respond quickly to customer issues (see Figure 29: Support and Escalation).

BCG provides direct access to product engineers if requested by a customer through the help desk. This streamlines the support process, eliminating the need to progress through multiple tiers of support to obtain problem resolution. All BCG Team engineers are equipped with the skill set required to adequately troubleshoot, and diagnose issues. It is the BCG Team’s assumption that help requests that are submitted by users would be collected and vetted by the State’s system administrators before escalation to the BCG Support Team. All BCG support team staff are full time employees of BCG based out of our USA offices.

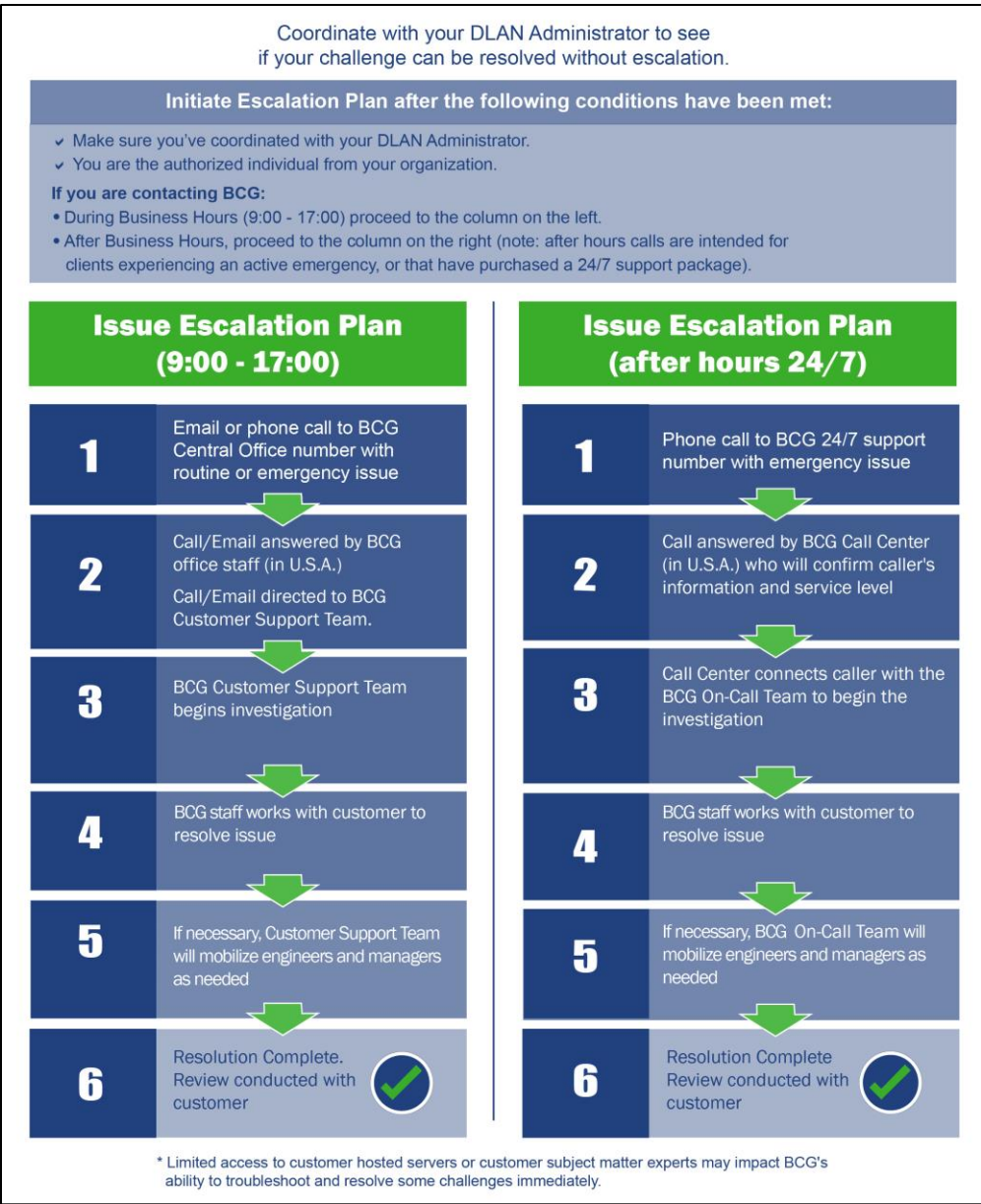


Figure 29: Support and Escalation

4.2.1.3.34 *The Vendor shall provide a proposed EMIS maintenance schedule and services schedule with costs and any additional service packages.*

BCG provides a required maintenance and support package for each DLAN system that entitles the customer to receive all updates to the software, including new versions, at no extra licensing cost. All DLAN versions are forward and backwards compatible by design and legacy data is always protected and supported. BCG uses an agile development methodology for DLAN and typically has updates available every 8-10 weeks. The state can choose how often they want to accept these DLAN updates, but BCG recommends at least bi-annually or annually. For security and support reasons, typically BCG does not support legacy versions of the software under standard maintenance for more than two years from date of issue unless specifically stipulated in a contract.

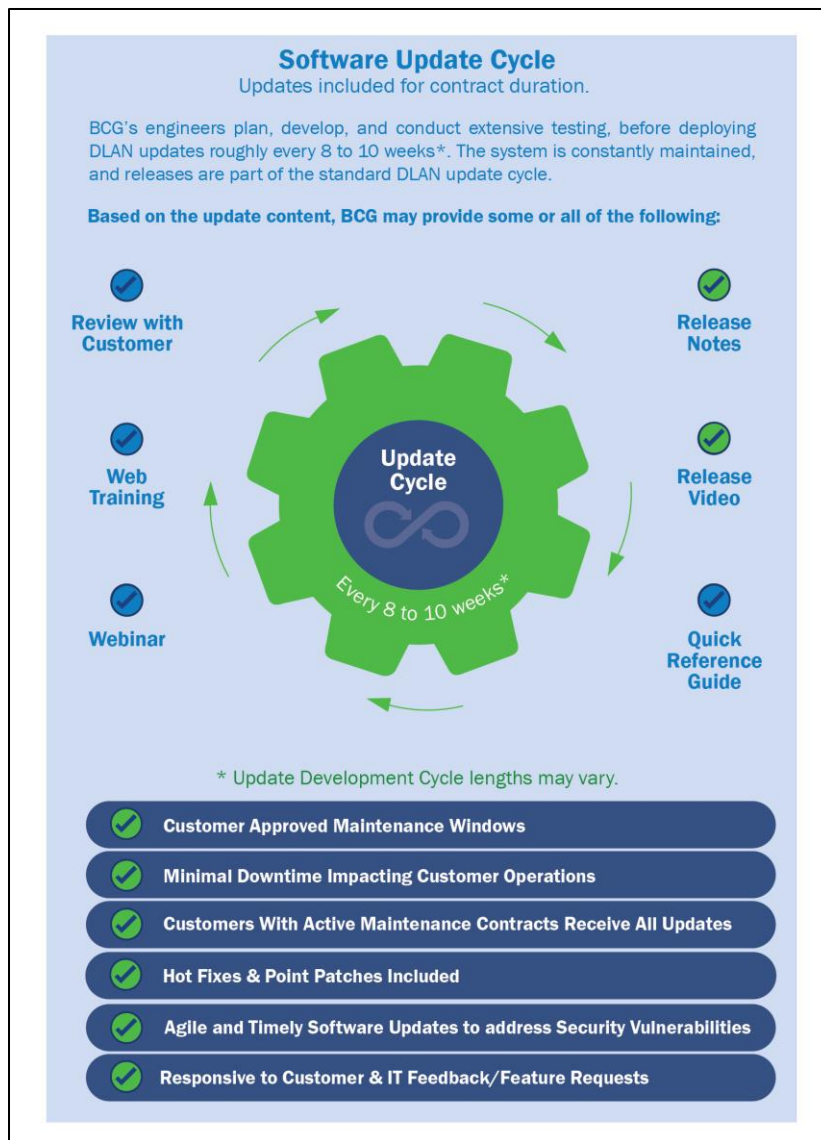


Figure 30: Continuing Support Cycle

4.2.1.3.35 *The EMIS shall provide a cyber-secure environment and a continuity plan in case of a system failure*

DLAN provides a cyber-secure environment and a continuity plan for all hosted systems. DLAN supports multi-node configurations, virtualization, high availability, load balancing, and disaster recovery. DLAN is also a secure solution and follows guidelines for NIST 800-53 and NEIM. BCG is also ISO 27001 certified. DLAN receives regular security and penetration testing by multiple customers per year. All tests are run by reputable third parties and BCG works with customers to address any potential threats in an expedited manner.

4.2.1.3.36 *The Vendor shall provide 24/7 technical support to sustain continuous operation. Vendor must provide support by telephone, online, and email 24 hours a day, 7 days a week, 365 days a year for troubleshooting technical issues.*

BCG is providing our 24/7 Gold Plus Level Support as described above (**Gold Plus Support**), including 24x7x365 access to BCG technical support team members through email, web, and telephone.

The Vendor will provide the following response times to request for technical support:

- 1. No more than one (1) business day for non-critical issues.*

BCG agrees to respond to requests for non-critical issues within (1) business day.

- 2. No more than two (2) hours for critical issues.*

BCG agrees to respond to requests for critical issues within (2) hours.

BCG's response service levels typically exceed what is asked for here. For additional service level information, please refer to BCG's service level chart, which is located in the Master Services Agreement on page 115.

4.2.1.3.37 The EMIS will be hosted on a minimum of a Tier 3 Data Center and have cloud-based hosting. Upon Agency request, the vendor shall provide a minimum of a Tier 3 data center certification verifying that it meets the following standards:

- 1. ISO 27001*

BCG has successfully completed the process of certification for ISO 27001, along with our HIPAA certification. In addition, BCG's engineers and quality assurance teams check all code against industry best practices including OWASP and SANS' top twenty list. BCG also maintains a disaster recovery and business continuity plan based on NIST 800-34r1. BCG's standard cloud datacenters perform SSAE 16 SOC2 Type II audits annually. They have achieved ISO 9001:2008, 27001:2013 and PCI 3.0 certification.

- 2. NIST SP800-53.*

BCG's business practices and the DLAN Product are in line with the controls listed in NIST SP 800-53. BCG works annually with third party security consultants to review our NIST SP800-53 controls and ensure we remain compliant and all practices are in line with the standard. This is in addition to our ISO 27001 certification.

4.2.1.3.38 The EMIS must be capable of being hosted on a minimum of a Tier 3 Data Center with a combination of local servers at the agency and have cloud-based hosting.

BCG uses Tier 3 or better Data Centers for all cloud hosting services. For this project, BCG proposes an Amazon Web Services (AWS) based cloud hosting solution managed by BCG and long-time datacenter partner Lumen.

Lumen

Lumen offers high-availability application hosting. Lumen offers a number of service options which include high SLAs, failover and redundancy. Servers will be in a secured facility (24/7/365). These facilities have enhanced security measures such as key card access, a secondary biometric authentication and video surveillance. Each data center holds several certifications and compliances (e.g. PCI DSS, SOC 2 TYPE II). A list of security features, certifications and compliances for a particular data center can be provided upon request.

Other Cloud Platforms

If Amazon Web Services cloud hosting is not desirable, BCG will work with your IT team to find a hosting platform that will meet your specific needs. In addition to our main hosting partners, BCG can also provide hosting through Microsoft Azure, Lumen, and other providers.

Additional Services

In addition to our base hosting packages, DLAN can provide a number of additional services including higher SLAs, disaster recovery, dedicated hardware, and additional surge capacity. BCG can work with your IT team to find a hosting environment that will meet your specific needs.

4.2.1.3.39 Vendors must provide a detailed response for each section in the specifications on how they meet or exceed the mandatory requirements. Vendors who fail to provide the required specification sheets within the allotted timeframe will be disqualified. This will require EACH SPECIFICATION to be detailed in bid submission. This shall be submitted as a WORD document or EXCEL document.

BCG has provided a detailed and thorough response to each section and requirement in the specifications list.

4.2.2 Contract Item 1: Annual Subscription for EMIS Solution

4.2.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.

BCG shall provide an annual cloud-based subscription for the DLAN EMIS solution it is proposing.

4.2.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per Section 4.1.1.3.10.

BCG shall provide access to the system for an estimated 500 concurrent users (accessing the EMIS simultaneously). The system also provides scalability, allowing WVDEM to add more users without delay or need to contact BCG for an increase in user accounts. If WV needs additional cloud resources for a sustained surge in the number of concurrent users they can contact BCG Support and make the request.

4.2.2.3 Vendor must provide the following with the annual subscription:

4.2.2.3.1 Maintenance and support services.

BCG will provide for ongoing update and maintenance of the system. This will include any bug fixes and updates that take place during the contractual period. BCG will coordinate any software updates and hardware maintenance with WVDEM to minimize impact to daily ongoing operations. If WVDEM is experiencing an emergency, they can request that BCG hold any updates until concluded.

4.2.2.3.2 Module customization, and setup.

BCG will configure the DLAN system to match WVDEM's desired status boards, forms, workflows, and settings to meet the State's needs. BCG will configure the software to match the desired State EOC organizational structure and operations. BCG will also work with WVDEM to identify key workflows, reporting requirements, communication chains, and system outputs and then configure the system in a way to meet these needs. BCG will

work with WVDEM IT to configure accounts, roles, and security rights for administrative personnel end users. System configuration is a process that occurs over several weeks with knowledge transfer and demonstrations between BCG and WVDEM. BCG will complete most configuration remotely. BCG will also review configuration settings with WVDEM and ask for sign-off of the final system configuration.

4.2.2.3.3 Onboarding for all users.

BCG shall provide onboarding services for WVDEM. A typical example of the onboarding process is below.

Example Standard Implementation Process	
BCG Responsibilities	Customer Responsibilities
 <p>Pre-Planning</p> <ul style="list-style-type: none"> ✓ BCG reviews pre-planning requirements with the customer, and secures all contacts needed. 	<p>Pre-Planning</p> <ul style="list-style-type: none"> ✓ Complete needs analysis ✓ Provide paper process and forms needed ✓ Identify challenges ✓ Outline technologies and integrations ✓ Identify user roles and responsibilities
<p>1</p> <p>Phase 1 - Planning</p> <ul style="list-style-type: none"> ✓ Host kick-off meeting ✓ Establish Project plan ✓ Design workflows 	 <p>Establish Steering Committee</p> <ul style="list-style-type: none"> ✓ Define project guidance and sponsorship ✓ Buy-in and sign-off ✓ Conduct executive review ✓ Identify security groups
<p>2</p> <p>Phase 2 - Configuration</p> <ul style="list-style-type: none"> ✓ Install and test application ✓ Configure dashboards and system ✓ Implement integrations ✓ Provide BCG's specialized knowledge transfer to working group (i.e. IT, GIS) 	 <p>Engage Working Group</p> <ul style="list-style-type: none"> ✓ Inform knowledge transfer and configuration ✓ Compose a working group of key staff (i.e. SMEs, managers, section chiefs, key stakeholder partners, and departments) ✓ Define the working process (day-to-day operations and emergency response) ✓ Identify views for exec, operations, and field
<p>3</p> <p>Phase 3 - Training</p> <ul style="list-style-type: none"> ✓ Distribute training plan and materials ✓ Conduct UAT, security scans, performance test (if needed) before training ✓ Complete user and admin training • Conduct exercise scenario (optional add-on) • Provide after action review (optional add-on) 	 <p>Working Group</p> <ul style="list-style-type: none"> ✓ Conduct UAT, security scans, performance test (if needed) before training ✓ Identify training levels and attendees ✓ Determine if training is on-site, remote, or hybrid ✓ Approve training deliverables
<p>4</p> <p>Phase 4 - Deploy System</p> <ul style="list-style-type: none"> ✓ Sign-off and go live ✓ Continuous support 	 <p>Working Group Becomes User Group</p> <ul style="list-style-type: none"> ✓ Sign-off and go live ✓ Continuous operations

Each customer implementation has unique parameters. Changes to the implementation process or requirements may affect the above example.

Figure 31: Implementation Process Example

In addition to onboarding, BCG has allocated for up to 8 days of onsite instructor-led training by BCG trainers. BCG can provide flexible topics and training plans tailored to fit WVDEM's organization. BCG will provide the following training materials: Quick Reference Guides for system administrators, basic users, and advanced users. BCG will also provide a training agenda document to assist WVDEM in scheduling their training activities, Micro-training videos designed for just in time training, and recording of all onsite instructor led training classes to assist with future staff onboarding.

4.2.2.3.4 Continuous access to training for all users.

BCG can provide continuing access to training for all users through both an annual instructor led refresher training and self-help services. For individuals looking to educate themselves at their own pace, BCG offers a built-in Online Help system with 375 user focused articles covering all topics in the system. Additionally Quick Reference Guide training materials and links to training videos will be loaded into the system for users to review.

4.2.2.4 Vendor must sign and return the attached Software as a Service Addendum prior to award of the contract.

This document is signed and attached in section [11.2 Software as a Service Addendum](#) below on page 88.

4.2.3 Acceptance of System

4.2.3.1 If the test period produces no issues at a minimum, the Agency will issue a Letter of Acceptance of the system, and the contract and annual license would start at that time.

BCG agrees to an acceptance period for the system. The contract and annual license will not start until the system has been accepted.

11. MISCELLANEOUS

11.1 Contract Manager

Contract Manager:	Gary F. Masterson
Telephone Number:	(716) 822-8668
Fax Number:	(716) 822-2730
Email Address:	gmasterson@bcgeng.com

11.2 Software as a Service Addendum

See attached

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
 - 10 days after the effective date of termination, if the termination is in accordance with the contract period
 - 30 days after the effective date of termination, if the termination is for convenience
 - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction) of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: WV Emergency Management Division

Signature: _____

Title: _____

Date: _____

Name of Vendor: Buffalo Computer Graphics, Inc

Signature: Ray J. Mustera

Title: PRESIDENT

Date: 3-Dec-2021

APPENDIX A

Version 11-1--19

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: BUFFALO COMPUTER GRAPHICS, Inc.

Name of Agency: West Virginia Emergency Management Division

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes
No
2. If yes to #1, does the restricted information include personal data?
Yes
No
3. If yes to #1, does the restricted information include non-public data?
Yes
No
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes
No
5. Provide name and email address for the Department privacy officer:
Name: PATRICK LUPIANI
Email address: PLUPIANI@bcgeng.com

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:
Name: PATRICK LUPIANI
Email address: PLUPIANI@bcgeng.com
Phone Number: 716 822 8668

EXHIBIT A – PRICING

**EXHIBIT A – Pricing Page
Emergency Management Information System
CRFQ 0606 HSE2200000005**

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Initial Year	Annual	1	\$263,021.01	\$263,021.01
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 2	Annual	1	\$126,828.59	\$126,828.59
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 3	Annual	1	\$126,828.59	\$126,828.59
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 4	Annual	1	\$126,828.59	\$126,828.59
Overall Total Cost				\$643,506.78	-

Please note: This information is being captured for auditing purposes.

Any product or service not on the Agency provided Cost Sheet will not be allowable. The state cannot accept alternate pricing pages, failure to use Exhibit A Cost Sheet could lead to disqualification of vendors bid.

Quantities listed herein are for bid evaluation purposes; no guarantee of any actual order quantities should be implied.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

BIDDER /VENDOR INFORMATION:

Vendor Name:	BUFFALO COMPUTER GRAPHICS, Inc.
Address:	4185 BAYVIEW RD.
City, St. Zip:	BLASDELL, NEW YORK 14219
Phone No.:	716-822-8668
Email Address:	RFPTeam@BCGENG.COM

Gary D. Masterson

Vendor Signature:

21-Dec-2021

Date:



SIGNED PURCHASING AFFIDAVIT

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Buffalo Computer Graphics, Inc

Authorized Signature: Ray J. Masterson Date: 3-Dec-2021

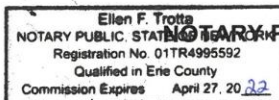
State of New York

County of Essex, to-wit:

Taken, subscribed, and sworn to before me this 3rd day of December, 2021.

My Commission expires April 27, 2022.

AFFIX SEAL HERE



Ellen F. Trotta

Purchasing Affidavit (Revised 01/19/2018)

SAMPLE BCG MASTER SERVICES AGREEMENT

BCG MASTER SERVICES AGREEMENT (MSA)

Updated 12/21/2021

This is a Master Services Agreement effective as of the Effective Date (as defined below) between: _____, a company having its principal place of business at _____ (the "Client") - AND -

Buffalo Computer Graphics, Inc., a company incorporated pursuant to the laws of the State of New York having its principal place of business at 4185 Bayview Road, Blasdell, New York 14219 ("BCG" or "Buffalo Computer Graphics").

For valuable consideration, the receipt and sufficiency of which is acknowledged, Client and Buffalo Computer Graphics (collectively, the "Parties" and each a "Party") agree as follows:

Composition of Agreement

This Master Services Agreement (including all exhibits attached hereto) ("**MSA**") is effective as of the date that the last Party executes this MSA (the date as indicated on the execution page of this MSA) (the "**Effective Date**"). The "**Agreement**" includes this MSA, the SLA, any Order Form(s) and/or Statement(s) of Work ("**SOW**"), the Acceptable Use Policy, which together constitute the entire agreement between the Parties with respect to the subject matter hereof and supersedes all proposals and prior discussions and writings between the Parties with respect thereto.

In the event of a conflict between the terms and conditions of the terms and conditions of any document comprising a part of the Agreement, the order of precedence shall be as follows:

- a) Exhibit A ("Acceptable Use Policy");
- b) this MSA;
- c) Exhibit E ("MSA/SLA Amendments");
- d) Exhibit D ("BCG Service Level Agreement");
- e) The applicable Terms and Conditions;
- f) The Order Form and/or SOW, unless either Order Form and/or SOW specifically states that a provision is to take precedence over a particular document; and
- g) All other exhibits.

1. Definitions

"**Acceptable Use Policy**" or "**AUP**" means the principles, rules and regulations that govern the use of the Services by Client as stated in the Buffalo Computer Graphics Policies attached hereto as Exhibit "A";

"**Bandwidth**" means the range of data transfer speeds measured in bits per second that a network can use. The greater the Bandwidth, the more information can be transferred over that network at one time.

"**Billing Commencement Date**" means (as applicable) the date specified on the Order Form or SOW or, if not specified, the date on which:

- a) Client is notified that Buffalo Computer Graphics is ready to accept the Client Hardware in the case of a Colocation Service;
- b) the operating system has been installed and the Managed Service is ready to accept Client's data in the case of a Managed Service; or
- c) two (2) months after the Effective Date if (a) through (b) above have not yet transpired.

"**Carrier**" means the company contracted by Buffalo Computer Graphics to supply telecommunications facility to the Client location on behalf of Buffalo Computer Graphics.

“Confidential Information” means all trades secrets and other proprietary information owned or licensed by one of the Parties or by any company affiliated with one of the Parties. Confidential Information includes, without limitation, licensed software, all feature sheets, pricing information, inventions, processes, algorithms, source code, client lists, financial information, legal, compliance, corporate, marketing, personnel, product, research, and other non-public information, in whatever form or media. Notwithstanding the foregoing, “Confidential Information” shall not include information which:

- (a) is or becomes generally available to the public other than as a result of its disclosure by the receiving Party or its representatives in breach of this Agreement or which the receiving Party knows (or ought reasonably to have known having made reasonable enquiry) to have been in breach of any other undertaking of confidentiality addressed to the disclosing Party (except that any compilation of otherwise public information in a form not publicly known shall nevertheless be treated as Confidential Information),
- (b) was lawfully in the possession of the receiving Party before the information was disclosed to it by the disclosing Party and continues to be held in accordance with the terms on which it was obtained,
- (c) the receiving Party can establish, through documentary evidence, was developed by or on behalf of the receiving Party without reference to any information disclosed by the disclosing Party, or
- (d) was authorized for release by the disclosing Party in writing.

“Custom Application” is applicable only in the context of a Managed Service and means those computer programs, including documentation relating thereto, all updates and new releases thereof, owned by or licensed to Client by a third party that are not included as part of the Managed Service. Buffalo Computer Graphics is not responsible for support nor licensing such Custom Applications.

“Client Data” means any data, content or information of Client or its end users that is stored, transmitted, or otherwise processed using the Buffalo Computer Graphics Services. BCG’s obligations with respect to such Client Data shall be exclusively governed by the Data Protection and Privacy Policies and are further subject to all Limitation of Liability provisions of this Agreement.

“Client Hardware” means the computer systems, peripherals, terminals, communications equipment and all other related hardware products owned or leased by, or otherwise under the control of Client as stated in the Client Hardware Inventory Form that has been approved by Buffalo Computer Graphics. Furthermore, any changes to this inventory are the responsibility of the Client to provide advanced written notice to Buffalo Computer Graphics on a go forward basis.

“Client Software” means the operating systems and applications, including documentation relating thereto, all updates and new releases thereof, owned by or licensed to Client by a third party that have been specifically approved by Buffalo Computer Graphics for inclusion as part of the Client System but not specifically identified by a Buffalo Computer Graphics Managed Services contract for support by Buffalo Computer Graphics. Furthermore, Buffalo Computer Graphics will not be responsible for licensing nor maintaining this software.

“Client System” means collectively the Client Hardware, Client Software, Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software, all as set out in the Order Form for a Managed Service.

“Facility” means a Buffalo Computer Graphics data center as specified in the Order Form.

“Fees” has the meaning set out in Section 4.1 of this MSA.

“Intellectual Property Rights” means, in respect of any technology, materials, content, or information, all

- (a) worldwide proprietary rights, now or hereafter in force or recognized, provided under
 - i. patent law,
 - ii. copyright law,
 - iii. trademark law (including laws creating rights in Internet domain name registrations),
 - iv. design patent or industrial design law,
 - v. semi-conductor chip or mask work, or
 - vi. any other applicable statutory provision or common law principle, including trade secret law, that may provide a right in such technology, materials, content, or information or the expression or use thereof, and
- (b) applications or registrations, or rights to apply for or obtain registrations, in respect of any of the foregoing.

"Leased Hardware" or **"Buffalo Computer Graphics Hardware"** means any servers, network appliances (e.g., Firewalls, IPS, Storage devices, etc.) utilized by Buffalo Computer Graphics to deliver services to Client.

"Licensed Software" or **"Buffalo Computer Graphics Software"** means any first and/or third-party licenses (e.g., DLAN Software, SQL licenses, Windows OS, etc.) utilized by Buffalo Computer Graphics to deliver services to Client.

"Maintenance Window" means a period of time designated in advance (on a standard recurring or emergency basis) by Buffalo Computer Graphics staff, during which preventive maintenance that could cause disruption of Service may be performed.

"Managed Service" means a data center hosting arrangement where Buffalo Computer Graphics provides all of the components (including both hardware and software) of Client's System to Client and, in addition to providing Facility Services, will install Client's System and will generally configure, back-up, secure and maintain all or a portion of Client's System. On an ongoing basis, Buffalo Computer Graphics ensures the system is up and running in its current state and applies security hot fixes and/or patches for managed applications as considered required by Buffalo Computer Graphics. Application version upgrades and downgrades, unless specifically requested by Buffalo Computer Graphics, are not included in the standard Managed Service arrangement.

"Marks" has the meaning set out in Section 2.13 of this MSA.

"MRC" means monthly recurring charge.

"Network" means the collection of Client locations connected by Buffalo Computer Graphics via one or more Carrier connections so as to enable telecommunications capabilities between such locations and the Facility.

"NRC" means non-recurring charge.

"Order Form" means any Order Form that references this MSA and is executed by both Parties hereto detailing the Buffalo Computer Graphics services requested by Client and agreed to by Buffalo Computer Graphics.

"Services" means the initial and subsequent Buffalo Computer Graphics service(s) provided to the Client as per an Order Form.

"Service Levels" means the predetermined, objective performance criteria for delivery of the Services as stated in the Buffalo Computer Graphics policies.

"Service Level Agreement" or "SLA" means, with respect to a specific Service, a level of performance at which Buffalo Computer Graphics is contractually obligated to deliver the Service to Client and which, depending on the specific Service ordered, is established with reference to certain metrics. If applicable, such metrics are outlined in the attached Service Level Agreement.

"Statement of Work" or "SOW" means the document which defines project-specific activities and deliverables for the Service(s) specified on the Order Form.

"Term" means the duration of time for which the Service is contractually committed. Such duration is indicated in the Order Form or SOW and starts on the Billing Commencement Date.

Any other capitalized term not defined in this MSA shall have the meanings set out in the Terms and Conditions or Schedules, as applicable.

2. General

2.1 Headings. Section headings are provided for convenience of reference only and do not constitute part of the Agreement. Any references to a particular section of this Agreement shall be deemed to include reference to any and all subsections thereof.

2.2 Severability and No Waiver. If any provision of the Agreement is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force without being impaired or invalidated in any way. The Parties agree to replace any invalid provision with a valid provision that most closely approximates the spirit and intent of the invalid provision. The waiver by either Party of a breach of any provision of the Agreement will not operate or be interpreted as a waiver of any other or subsequent breach.

2.3 Assignment. Client may not assign nor delegate any or all of its rights or its duties or obligations under this Agreement without the prior written consent of Buffalo Computer Graphics; provided, however, that Client may, without the prior written consent of Buffalo Computer Graphics, assign this Agreement to an affiliate of Client or to a successor of all or substantially all of the assets of Client through merger, reorganization, consolidation or acquisition. Notwithstanding the foregoing, BCG may increase the Fees if BCG determines, in its sole, reasonable discretion, that an assignment materially increases BCG's cost of providing the services.

2.4 Independent Contractors. The Parties to the Agreement are independent contractors, and no agency, partnership, joint venture or employment relationship is intended or created hereby. Neither Party shall have the power to obligate or bind the other Party. Personnel supplied by Buffalo Computer Graphics shall work exclusively for Buffalo Computer Graphics and shall not for any purpose be considered employees or agents of Client.

2.5 Subcontractors. Buffalo Computer Graphics shall be fully responsible for the performance of all of its obligations under this Agreement, including any obligations performed by a subcontractor.

2.6 Notices. All notices, requests, demands or communications required or permitted hereunder shall be in writing, and delivered by one or more of the following methods (with recognized receipt date):

- a) personally (when delivered)
- b) electronic transmission / email (when acknowledged as received by recipient; note: automatic response does not constitute acknowledgement)
- c) certified or registered mail to the respective addresses as set forth below or at such other addresses as shall be given in writing by either Party to the other (when received and signed for).

2.7 Governing Law, Jurisdiction and Venue. The Agreement created hereunder shall be deemed to have been made in, and shall be construed pursuant to, the laws of the State of New York and any action or proceeding arising out of or related to this Agreement shall be brought only in the federal or state courts located in the State of New York. The Parties hereby irrevocably consent to such jurisdiction and venue.

2.8 Counterparts. The Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

2.9 Force Majeure. "Force Majeure" means an event, the cause of which is beyond the reasonable control of the Party affected thereby and which could not reasonably have been foreseen and provided against, including, without limitation, acts of god, strikes, lock outs or other labor or industrial disturbances, accidents, fires, explosions, interruptions in telephone, electrical, cable, fiber or other services necessary to perform the Services, weather conditions materially preventing or impairing work, inability to secure fuel, power, materials, contractors or labor, mechanical breakdown, failure of equipment or machinery, delays in transportation, wars, civil commotion, riot, sabotage, applicable legislation and regulations thereunder, interruption by government or court orders and future orders of any regulatory body of competent jurisdiction. Notwithstanding any other provision of the Agreement, if by reason of Force Majeure, either Party is wholly or partly unable to perform certain elements of its obligations hereunder, it shall be relieved of those obligations to the extent, and for the period, that it is affected by Force Majeure, provided that the affected Party gives the other Party prompt notice of such inability. The Party affected by Force Majeure shall use all reasonable efforts to remedy the situation and remove, so far as possible and with reasonable speed, the cause of its inability to perform, provided that there shall be no obligation on a Party so affected to settle labor disputes or to test or to refrain from testing the validity of any order, regulation or law in any court having jurisdiction.

2.10 Non-Solicitation. Both Buffalo Computer Graphics and Client agree that during the Term of this Agreement and for a period of one (1) year following the expiration or termination hereof, neither Party shall, directly or indirectly, hire or offer to hire or entice away or in any other manner persuade or attempt to persuade any officer, employee, agent, or client of the other Party to discontinue his or her or its relationship with the other Party. A general advertisement or notice of a job listing or opening or other similar general publication of a job search or availability to fill employment positions, including on the internet, shall not be construed as a breach of this Section and the hiring of any such employees or independent contractor who freely responds thereto shall not be a breach of this Section.

2.11 Amendments. No amendment, modification, supplement or other purported alteration of this Agreement shall be binding upon a Party unless in writing signed by them or on their behalf by a duly authorized representative(s).

2.12 Survival. Sections 2.2, 2.7, 2.10, 2.12, 3.5, 4, 5 and 6 shall survive the expiration or termination of this Agreement along with any other provision of this Agreement which expressly states it is to continue in effect after termination or expiration of this Agreement.

2.13 No Lease. The Parties acknowledge and agree that this Agreement is a services agreement and is not intended to and shall not constitute a lease of or tenancy or other interest in the Facility, any real property owned or leased by Buffalo Computer Graphics or in any Buffalo Computer Graphics Hardware or any other personal property of Buffalo Computer Graphics.

3. Delivery and Term

3.1 Delivery of Services. Subject to Client's compliance with the Acceptable Use Policy (AUP), a copy of which is attached as Exhibit "A", and the Credit Application Form, Services are acquired from Buffalo Computer Graphics by using Order Form(s) and/or SOW(s). Each Order Form and/or SOW shall be on Buffalo Computer Graphics' standard form and must be executed by both Buffalo Computer Graphics and Client prior to becoming effective. Upon each Order Form and/or SOW becoming effective, it shall, along with the applicable Terms and Conditions and the Schedules referenced therein, form a part of this Agreement and be governed by the terms and conditions contained herein. For greater certainty, Client agrees to be bound by this MSA and the applicable Terms and Conditions during the provisioning period, which is defined as the period from the Effective Date to the commencement of the Initial Term. In the event that Buffalo Computer Graphics is unable to provision a particular Service due to lack of Service availability, Client will not be responsible for the payment of such Service and Buffalo Computer Graphics will not be responsible to Client for any costs Client may have incurred in preparation for Service implementation. Client will continue to be bound by this Agreement for all provisioned Services.

BCG hereby grants Client a non-exclusive, non-transferable (except in compliance with Section 2.3) right for Client and its affiliates to access and use the Services during the Term. Such use is for Client and its affiliates' internal use.

3.2 Term and Renewal. Services for which the Order Form and/or SOW states a "Total Recurring Fee" shall commence on the Billing Commencement Date and shall continue for the duration of the Term set out herein (the "Initial Term") unless otherwise terminated as set forth in this Agreement. Such Services shall automatically renew for additional successive terms of equal duration to the Term (the "Renewal Term") unless either Party delivers to the other Party written notice of its intention not to renew the Agreement no less than ninety (90) days prior to the expiration of the Initial Term or Renewal Term, as applicable.

3.3 Client's Termination with Cause. Notwithstanding anything to the contrary contained in this Agreement, Client may terminate this Agreement effective immediately upon delivery of notice of termination to Buffalo Computer Graphics if Buffalo Computer Graphics becomes insolvent or bankrupt or makes an assignment for the benefit of creditors or appoints (or having appointed) a receiver or trustee in bankruptcy or upon the proceeding in bankruptcy, receivership or liquidation being instituted against Buffalo Computer Graphics and continuing for thirty days without being dismissed.

3.4 Buffalo Computer Graphics' Termination with Cause. Notwithstanding anything to the contrary contained in this Agreement, Buffalo Computer Graphics may, at its option and in addition to any other rights and remedies available at law or equity, terminate this Agreement:

- a) any time during the Suspension Period for any reason upon prior notice to Client;
- b) upon written notice to Client if Client materially breaches this Agreement and such breach is incapable of cure or, with respect to a material breach capable of cure, Client does not cure such breach within thirty (30) days after receipt of written notice of such breach;
- c) immediately upon Client becoming insolvent or bankrupt or making an assignment for the benefit of creditors or appointing (or having appointed) a receiver or trustee in bankruptcy or upon any proceeding in bankruptcy, receivership or liquidation being instituted against Client and continuing for thirty days without being dismissed.

3.5 Payment Upon Termination and Effect of Termination. Upon providing notice of termination of this Agreement for any reason whatsoever (or termination of an Order Form or SOW) Client shall immediately pay to Buffalo Computer Graphics:

- (a) any accrued liability or amount owing for the Services rendered but not yet paid up to the effective date of termination in the case of termination of the applicable Order Form or SOW; and
- (b) any balance of Fees due to the end of the then current Term for the terminated Service(s).

Within five (5) business days of Buffalo Computer Graphics' receipt of all final Fees following termination or natural expiry of the Term, Buffalo Computer Graphics will make available to Client the Client Hardware (containing the Client Software, Custom Application (as applicable) and Client's data). Client acknowledges and agrees that Buffalo Computer Graphics is under no obligation to make available the Buffalo Computer Graphics Software and shall be allowed to remove it from the Client Hardware except in the case where the software is migrated to an on-premises solution pursuant to a written agreement between the parties.

Upon termination of this Agreement, any credits to which Client is entitled resulting from Buffalo Computer Graphics' failure to meet its SLA's in the last calendar month during the Term, shall be paid out to Client by Buffalo Computer Graphics within 60 business days of the effective date of termination of this Agreement. This Section shall survive the expiry or termination of the Agreement.

3.6 Service Suspension and Access Restriction. Buffalo Computer Graphics may suspend or restrict the Services (in whole or in part), including but not limited to the Service Levels (the "**Suspension Period**"):

- a) any time after the 60th day after the date of any invoice in the event that Client has not paid the subject invoice in full;
- b) at any time if Buffalo Computer Graphics' operations are impaired by Client's use of the Service(s);

Buffalo Computer Graphics will promptly recommence the Services following the cure of the underlying issue. Notwithstanding any suspension of Service(s), Client shall remain liable for payment of all invoices through the entire Suspension Period

4. Fees and Payment

4.1 Fees. “Fees” shall mean any one or more fee, as may be applicable as stated in the Order Form and/or SOW, and any other fees charged by Buffalo Computer Graphics. Fees include the cost of third-party retail services or products (including increases thereto) upon written notice to Client, purchased by Buffalo Computer Graphics at the request of Client. Any additional, supplemental or upgrade Services may result in additional fees or other charges. Client may request expedited service installation, and if Buffalo Computer Graphics is able to accommodate such request, Buffalo Computer Graphics may charge additional reasonable fees associated with such request. Client certifies that all information provided to Buffalo Computer Graphics is complete and accurate. Any costs incurred by Buffalo Computer Graphics due to errors or omissions documented on an Order Form of SOW (whether written or electronic) will be charged back to Client. Invoices will be emailed on a monthly or annual basis (depending upon agreed upon payment terms), in advance, to the email address listed in this Agreement, or to such additional or replacement email address(es) as directed by the Client. If no email is listed, invoices will be mailed to the address on the first page of this Agreement. Invoices are due within 60 days of the invoice date, except that Client may withhold from any payment any charge or amount disputed in good faith by Client pending resolution of such dispute. Fees shall be payable without counter-claim, setoff or demand. All Fees, invoices and payments shall be in US dollars unless otherwise stated.

4.2 Reduced Services. If Client subsequently selects a smaller quantity of or downgrades any of the Services before the end of the Initial Term or any Renewal Term, Client will remain responsible for paying all Fees and charges for such original quantity and level of Services to the end of the Initial Term or Renewal Term (as applicable). Client acknowledges that this Section 4.2 is not intended as a penalty clause and represents a genuine estimate of the losses that would be incurred by Buffalo Computer Graphics due to the reduction or downgrade of Service.

4.3 Credit. Buffalo Computer Graphics may at any time perform a credit analysis of Client. Client shall provide any credit information reasonably requested by Buffalo Computer Graphics. Following such credit analysis, Buffalo Computer Graphics may, in its sole discretion, require Client to pay the total Fees, or any portion thereof, in advance of providing Services and/or require other assurances to secure Client’s payment obligations under this Agreement.

4.4 Taxes. In addition to the Fees, Client shall be responsible for paying any applicable sales, use, excise, value added or similar sales taxes or assessments imposed upon the Services by any federal, provincial/state, or local government authority, exclusive of taxes based upon Buffalo Computer Graphics’ income or payroll.

4.5 Interest. Interest shall begin to accrue on unpaid invoices after thirty (30) days of the date of each invoice at the rate of the lower of 1.5% per month (18% per year) or the maximum permitted by law until paid in full.

4.6 Fee Increases and Renewal. Buffalo Computer Graphics may increase the Fees for any Renewal Term upon not less than 120 days’ notice prior to the commencement of such Renewal Term. In addition, Buffalo Computer Graphics has the right to increase the Fees by the lesser of 2.5% of the preceding year’s Fee or the percentage increase in the national Consumer Price Index over the prior twelve-month period. Notwithstanding the foregoing, Buffalo Computer Graphics may increase the Fees at any time immediately upon notice to Client in the event of industry changes, which are beyond the reasonable control of Buffalo Computer Graphics, including without limitation, carrier pricing policy changes, telecommunications tariff changes, commodity price increases and foreign exchange fluctuations.

4.7 Disputes. Subject to Section 4.2 of this MSA, Client may reasonably dispute any Fees if, and only if, Client:

- a) presents a written statement of any billing discrepancies to Buffalo Computer Graphics in reasonable detail together with appropriate supporting documentation no later than 5 days after notifying Buffalo Computer Graphics of such dispute; and
- b) negotiates in good faith with Buffalo Computer Graphics for the purpose of resolving such dispute within ten (30) days of submitting such written statement to Buffalo Computer Graphics. In the event such dispute is mutually agreed upon and resolved in favor of Client, Client will receive a credit for the disputed Fees. In the event the dispute is not resolved in such thirty (30) day period, either Party may pursue any available remedies.

4.8 Currency. All references to currency in this Agreement are to U.S. dollars, unless otherwise stated in the Order Form.

4.9 Service Levels; Credits. Refer to the Service Level Agreement exhibit for details on BCG's SLA. The remedies set forth in BCG's SLA constitutes Client's sole and exclusive remedy for BCG's failure to satisfy the commitments in the SLA.

Service credits, if any, as provided in the SLA or any other credits Client may be eligible to receive for Services purchased pursuant to a valid promotion will be issued to Client's account during the Term of the Agreement. In the case where there will be no further invoices, BCG will pay the amount of the service credits to Client in cash, by check or wire transfer, within 60 days after the end of the Agreement.

5. Representations, Warranties, Liability and Indemnity

5.1 Buffalo Computer Graphics Representations and Warranties. Buffalo Computer Graphics represents, warrants and covenants as follows:

- a) it has obtained all licenses, permits and approvals from any and all governmental authorities required in respect of its properties and operations as presently owned and carried on and in respect of the performance of the Services;
- b) to its knowledge, it is under no obligation or restriction, nor will it assume any such obligation or restriction, which would in any way interfere or be inconsistent with, or present a conflict of interest concerning the performance of the Services;
- c) it will perform its obligations hereunder in a professional and workmanlike manner and in accordance with applicable industry standards or as may be stated in an SOW or an Order Form;
- d) the performance of Services will not violate or infringe on the Intellectual Property Rights, proprietary rights, or any other rights, of any person;
- e) in carrying out its obligations under this Agreement, it shall comply with the terms and conditions of any applicable open source software license(s);
- f) it is a corporation duly incorporated under the laws of New York and is validly subsisting under such laws and has all the necessary corporate power and authority to own its properties and to carry on its businesses as presently owned and carried on;
- g) it has the corporate power and authority to enter into and perform its obligations under this Agreement; and
- h) it has duly authorized, executed and delivered this Agreement, and this Agreement constitutes a valid and binding obligation enforceable in accordance with its terms.

EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, BUFFALO COMPUTER GRAPHICS HEREBY DISCLAIMS AND MAKES NO WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR AVAILABILITY, LACK OF NEGLIGENCE, SERVICES OR THAT BUFFALO COMPUTER GRAPHICS EQUIPMENT WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT ALL ERRORS CAN OR WILL BE CORRECTED OR THAT THE SERVICES OR BUFFALO COMPUTER GRAPHICS'S EQUIPMENT WILL FUNCTION IN CLIENT'S ENVIRONMENT, OR LOSS OF DATA. BUFFALO COMPUTER GRAPHICS DOES NOT PROVIDE ANY WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, AND CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT, WITH REGARD TO THE EQUIPMENT OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) PROVIDED IN CONNECTION WITH THIS AGREEMENT. IN THE EVENT OF ANY INTERRUPTION, FAILURE OR BREAKDOWN IN THE SERVICES, OR OF THE LOSS OR SPOILING OF THE CONTENT, BUFFALO COMPUTER GRAPHICS MAKES NO WARRANTY THAT EITHER WILL BE RESTORED. UNLESS OTHERWISE STATED IN THIS AGREEMENT, THE CLIENT ASSUMES FULL RESPONSIBILITY FOR BACKING UP ITS OWN FILES AND THE ENTIRE RISK AS TO THE QUALITY OF, OR ARISING OUT OF, USE OR PERFORMANCE OF THE SERVICES AND BUFFALO COMPUTER GRAPHICS EQUIPMENT REMAINS WITH CLIENT. CLIENT EXPRESSLY ACKNOWLEDGES THAT ALTHOUGH BUFFALO COMPUTER GRAPHICS USES COMMERCIALY REASONABLE EFFORTS TO ENSURE THE PROTECTION OF CLIENTS DATA, BUFFALO COMPUTER GRAPHICS DOES NOT PROVIDE OR GUARANTEE ABSOLUTE SECURITY.

5.2 Client's Representations and Warranties. Client represents, warrants and covenants (where applicable) that:

- a) it is the true and lawful owner or licensee of the Client Software and Custom Applications (as applicable) and has the full right and ability to use such Client Software and Custom Applications as contemplated in this Agreement;
- b) it has the right to place Client Hardware in the Facility for receipt of the Services as contemplated herein;
- c) its use of Buffalo Computer Graphics controlled IP Addresses or use of the Services including any data transmitted, stored or received will not
 - (i) violate any applicable laws, regulations or Buffalo Computer Graphics Policies,
 - (ii) cause a breach of any agreement with any third party, or
 - (iii) interfere with other Buffalo Computer Graphics Client's use of any Buffalo Computer Graphics services or Buffalo Computer Graphics' network;
- d) it shall throughout the Initial Term and any Renewal Terms, be solely responsible and liable for the proper configuration, operation and management of the Client Software or Custom Applications (as applicable) without any liability, express or implied, accruing to Buffalo Computer Graphics whatsoever; and
- e) it has, where applicable, obtained all necessary consents to conduct its business in compliance with the *Personal Information Protection and Electronic Documents Act* or other similarly applicable federal or provincial/state statute.

5.3 Limitation of Liability.

Except for claims arising from Section 5.4, Section 5.5 or Section 6 of this MSA and any claims specifically exempted in any Terms and Conditions attached hereto, neither Buffalo Computer Graphics nor Client shall be liable to the other under the Agreement in connection with any single event or series of events for any special, indirect, consequential, exemplary or punitive damages including, but not limited to, lost profits, lost business revenue, lost or damaged data, failure to realize expected savings, or other commercial or economic loss of any kind even if the other Party has been advised of the possibility of these losses or damages, and regardless of the form of action, whether in contract or tort, including negligence or based upon any other legal or equitable theory. Furthermore, Client agrees that Client's sole and exclusive remedy for Buffalo Computer Graphics' failure to provide the Services in accordance with the applicable Service Levels shall be as set out in such Service Levels. Except for claims arising from Section 5.4, Section 5.5 or Section 6 of this MSA, and any claims arising out of BCG's gross negligence or willful misconduct, in no event will Buffalo Computer Graphics' liability to Client, or to that of its directors, officers, employees or users of the Services exceed the Fees actually paid to Buffalo Computer Graphics for the affect Service(s) within the three (3) month period immediately preceding the date on which the cause of action arose, excluding Fees for Implementation Services as itemized in Exhibit C. Notwithstanding the foregoing, BCG's total cumulative liability for claims arising from Section 5.4, Section 5.5 or Section 6 of the MSA, and any claims arising out of BCG's gross negligence or willful misconduct, will not exceed the total fees paid to Buffalo Computer Graphics for the affected Service(s) within the six (6) month period immediately preceding the date on which the cause of action arose.

5.3 Indemnity. Indemnity as related to this MSA is as follows:

- a) If either Party (the "Indemnitee") promptly notifies the other (the "Indemnitor") of a third party claim against the Indemnitee that any of the Services or Client supplied hardware, software or data, as the case may be, infringes a presently existing proprietary right of a third party, and if the Indemnitee specifies in such notice that the claim is based to any extent upon an alleged infringement of any portion of the Indemnitor's properties (Services or Client supplied hardware, software or data, as the case may be), the Indemnitor, with respect to and to the extent of the portion of the claim pertaining to the Indemnitor's properties, shall indemnify and defend such claim at its expense and pay any costs or damages that may be incurred or finally awarded against the Indemnitee. THIS SECTION SETS FORTH THE COMPLETE LIABILITY OF THE PARTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.
- b) Client agrees that it shall indemnify, defend and hold BCG, its officers, directors, employees and contractors harmless from and against any and all claims, costs, liabilities and damages which arise from or relate to the indemnifying Party's failure to comply in the conduct of its business with the CAN-SPAM Act of 2003 (15 U.S.C. 103) and the Telephone Consumer Protection Act and other similarly applicable federal or state statute(s).

- c) Client shall indemnify, defend and reimburse Buffalo Computer Graphics for, and hold Buffalo Computer Graphics harmless from, any and all claims or lawsuits of any person and resulting costs (including reasonable attorney's fees), damages, losses, consequences, awards and judgments:
 - i. for breach of Section 5.2 or Section 5.5 of this MSA;
 - ii. based on the use by Client or any third party of Content retrieved from or produced by the Services;
or
- d) In the event that either Party institutes any legal suit, action, or proceeding against the other Party arising out of or relating to this Agreement, the prevailing Party in the suit, action or proceeding shall be entitled to receive, in addition to all other damages to which it may be entitled, the costs incurred by such Party in conducting the suit, action, or proceeding, including reasonable attorneys' fees and expenses and court costs.
- e) An Indemnitee's failure to give prompt notice of a claim under this Section 5.4 shall not relieve Indemnitor of its obligation to indemnify except to the extent that Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. Indemnitor may not settle any claim pursuant to this Section 5.4 unless it unconditionally releases Indemnitee of all liability and does not include an admission of wrongdoing, fault or liability on behalf of Indemnitee.

This Section 5.4 shall survive expiry or termination of the Agreement.

5.5 Privacy. Each Party shall comply with all applicable privacy or data protection laws, statutes and regulations, including without limitation, having a written privacy policy governing the collection, use and disclosure of Personal Information (as such term is defined in the applicable statute) and being in compliance with such privacy policy. Without limiting the foregoing, BCG shall comply with the California Consumer Privacy Act of 2018 ("CCPA") and BCG shall process Client's personal information solely as necessary to provide the Services under this Agreement and as otherwise necessary to perform its obligations under this Agreement. BCG may only process Client's personal information for the duration of this Agreement. BCG acknowledges that it has given no consideration (monetary or otherwise) for any disclosure or transfer of Client's personal information from Client to BCG. Any such Client personal information is provided for the sole purpose of facilitating the Services. BCG shall comply with all reasonable documented instructions of Client with respect to Client's personal information, and shall immediately inform Client if, in BCG's opinion, an instruction conflicts with applicable data privacy laws. With respect to personal information as that term is defined by Section 1798.140 of the CCPA ("CCPA PI"), BCG will not collect, sell, or use the CCPA PI except as necessary to perform the purpose specified in this Agreement, and BCG will retain, use, or disclose CCPA PI only for the specific purpose of performing BCG's obligations under the Agreement and not for any other purpose, including selling, retaining, using or disclosing the CCPA PI for a commercial purpose other than providing the Services specified in or for the intended purpose of this Agreement.

BCG will not disclose, modify, or access Client's Data, except (a) with Client's authorization to do so in connection with Client's use of the Services, including requests for support; or (b) as necessary to provide the Services to Client or to prevent or address service or technical problems, or to comply with this Service Exhibit; or (c) at the request of a governmental or regulatory body, subpoenas or court order.

Based on the Services provided to Client by Buffalo Computer Graphics, Client grants permission to Buffalo Computer Graphics (which consent includes the initial installation and all future updates, patches, software and hardware configurations) to install the following on Client's application hosting platform provided by BCG and/or data hosting partner:

For Clients using Services that are managed by Buffalo Computer Graphics:

- a) anti-virus software installed for anti-virus also known as software for anti-malware protection. This software is used to prevent, detect and remove malicious software;
- b) monitoring software installed for the maintenance and observation of the performance of servers and server resources. This software will communicate securely with Buffalo Computer Graphics' centralized monitoring infrastructure;
- c) Buffalo Computer Graphics may install custom scripts and/or applications on Client's equipment or Buffalo Computer Graphics rental equipment in support or Buffalo Computer Graphics service maintenance and monitoring solution, or for other purposes by Client request. These scripts may create logs and send out e-

mails as required. The logs may be collected by Buffalo Computer Graphics and used for maintenance and troubleshooting purposes; and

- d) software and or agents to perform Client data backup and restoration functionalities.

BCG will store the Client Data only in North America, unless Client provides written authorization for an alternate location. BCG or its affiliates' personnel located outside of the United States shall not access the Client Data, except with Client's prior written consent.

5.6 No Control. Client acknowledges that Buffalo Computer Graphics does not own or have any control over the content, availability, accuracy or any other aspect of any information, data, files, pictures or content in any form or any type ("Content") made accessible or available by or to Client or Client's end users through the use of the Services and Buffalo Computer Graphics does not monitor the use of the Services by Client or its end users except as provided in this Agreement. Client agrees that all Content that Client accesses through Buffalo Computer Graphics is accessed and used by Client at Client's own risk, and that Buffalo Computer Graphics will not be liable for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to Client access to such Content.

In cases where BCG integrates with or provides third-party data Content, BCG does not have any control over the content, availability, accuracy or any other aspect of any information, data, files, pictures or content in any form or any type ("Content") made accessible or available by such third-party Content. In the event that there is an issue with accessing third-party services/data, BCG will work in good faith to resolve access issues.

5.7 BCG Compliance and Security. Buffalo Computer Graphics will comply with all laws and regulations applicable to BCG's provision of the Service, and Client will comply with all laws and regulations applicable to Client's use of the Service. BCG has adopted and implemented, and will maintain, a corporate information security program designed to protect Client data from loss, misuse and unauthorized access or disclosure. Such program includes formal information security policies and procedures. The BCG information security program is subject to reasonable changes by BCG from time to time. In addition to BCG's obligations in the Agreement, BCG, as of the date of this Agreement, has obtained an AICPA sanctioned Type II audit report (i.e., SSAE18/ISAE3402 SOC 1 or AT-101 SOC 2) for the hosting data centers and intends to continue securing such audits pursuant to a currently sanctioned or successor standard. Client, upon written request and under confidentiality agreement, will be entitled to receive a copy of the then-available report, which is BCG Confidential Information.

5.8 HIPAA. To the extent the Services involve the ongoing storage of or routine access to PHI (as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, "HIPAA"), or BCG is otherwise acting as a Business Associate (pursuant to HIPAA), BCG will agree to the terms in its then-current Business Associate Agreement upon Client's request.

6. Confidentiality

6.1 If applicable, an NDA shall apply to this Agreement and is hereby incorporated by this reference except that for the purposes of this Agreement the term of the NDA shall be extended until the end of the Initial Term (or Renewal Term as applicable) in the event that the NDA expires prior to the end of the Initial Term (or Renewal Term) of this Agreement.

6.2 In the event an NDA has not been executed by Client and Buffalo Computer Graphics, the Parties agree to hold in strictest confidence, not to use and not to disclose to any third party any Confidential Information of the other party, without the prior written consent of such other Party. For purposes of clarification, Buffalo Computer Graphics will not be prohibited or enjoined at any time from utilizing any skills or knowledge of a general nature acquired during the course of providing the Services, including, without limitation, information publicly known or available or that could reasonably be acquired in similar work performed for another Buffalo Computer Graphics client.

6.3 Unless otherwise prohibited by law, if the receiving party becomes legally obligated to disclose Confidential Information, the receiving party will give the disclosing party prompt written notice sufficient to allow the disclosing party to seek a protective order or other appropriate remedy, and will reasonably cooperate with the disclosing party's efforts to obtain such protective order or other remedy at the disclosing party's expense, and in the event the receiving party is unable to do so, the receiving party will (so long as not prohibited by law from doing so) advise the disclosing party immediately subsequent to such disclosure. The receiving party will disclose only such information as is required, in the opinion of its counsel, and will use commercially reasonable efforts to obtain confidential treatment for any Confidential Information that is so disclosed.

6.4 All Confidential Information will remain the exclusive property of the disclosing party, and the receiving party will have no rights, by license or otherwise, to use the Confidential Information except as expressly provided herein. Upon the disclosing party's written request, the receiving party will promptly return or destroy, and verify in writing its destruction of, all material, in any form, embodying Confidential Information of the disclosing party. In carrying out any destruction, the receiving party will protect Confidential Information in accordance with the terms of this Agreement.

6.5 The receiving party acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to the disclosing party for which monetary damages may be difficult to ascertain or be an inadequate remedy. The receiving party therefore agrees that the disclosing party will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

7. General

7.1 Provision of Public IP Addresses. Buffalo Computer Graphics will assign, on a temporary basis, a number of Internet Protocol Addresses ("IP Addresses") that Buffalo Computer Graphics, in its sole discretion, considers reasonable. Client acknowledges that

- a) IP Addresses are assigned as part of the Services and are not portable and
- b) Client does not obtain any right or title to assigned IP Addresses. Buffalo Computer Graphics reserves the right to change IP Address assignments at any time, provided Buffalo Computer Graphics uses reasonable commercial efforts to avoid disrupting the Services. Client agrees that any renumbering required of Client after termination of this Agreement shall be the sole responsibility of Client.

7.2 Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software.

- a) **Title.** Title to the Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software remains with Buffalo Computer Graphics or its suppliers, as the case may be and, except as expressly granted hereunder, no right title or interest in or to the Buffalo Computer Graphics Hardware or Buffalo Computer Graphics Software passes to Client. Accordingly, Client shall not dispose of or suffer a lien or encumbrance upon the Buffalo Computer Graphics Hardware or Buffalo Computer Graphics Software. Client further agrees to not
 - i. modify any part of the Buffalo Computer Graphics Software,
 - ii. translate, decompile, disassemble, decrypt, reconstruct, or reverse engineer the Buffalo Computer Graphics Software,
 - iii. remove any proprietary notices, labels or marks from the Buffalo Computer Graphics Software or Buffalo Computer Graphics Hardware,
 - iv. authorize or acquiesce in the use of the Buffalo Computer Graphics Software by persons other than Client and Buffalo Computer Graphics, and
 - v. copy the Buffalo Computer Graphics Software or documentation.
- b) **Leased Terms.** Client may not remove any item of Leased Hardware or Licensed Software from the Facility or Client location (whatever the case may be) and, unless otherwise agreed in writing by Buffalo Computer Graphics, may use the Leased Hardware and Licensed Software only for the purpose of delivering the Services. Buffalo Computer Graphics may replace items of Leased Hardware and accessories from time to time provided that it gives written notice to Client and that any such replacement does not substantially diminish the technical parameters of the Service. Buffalo Computer Graphics is not responsible for replacement of end of life hardware until support for such hardware is no longer available by the manufacturer, at which time replacement hardware will be as per manufacturer specifications. If any Leased Hardware or Licensed Software is damaged as a result of any act or omission of Client (including its agents, consultants or clients), Client shall compensate Buffalo Computer Graphics for the damage including any additional costs of repair incurred by Buffalo Computer Graphics.

7.3 Escalation Procedures. Buffalo Computer Graphics' current technical support escalation procedures are provided in the table below. All issues are responded to as quickly as possible in order to restore services and minimize downtime. BCG will work with the Client to determine the Severity and Impact of the reported issue based on the impact on business operation.

Problem Severity	Severity Code	Impact	Description and Resolution Support Requirement
1	Critical	Mission Critical	System is not operational/unavailable/significant measurable performance degradation: BCG will commit a full-time resource, or team of resources, to resolve the problem as soon as possible. All efforts will be made to resolve the issue within a twenty-four (24) hour period.
2	High	Major	Critical functionality is not operational: BCG will commit a full-time resource, or team of resources, during normal business hours to resolve the issue as soon as possible. All efforts will be made to resolve the issue with a forty-eight (48) hour period.
3	Medium	Moderate	Non-critical functionality is not operational: BCG will commit a resource, or team of resources, during normal business hours to restore service to a satisfactory level. All efforts will be made to resolve the issue within five (5) business days.
4	Low	Minor	Specific issue or questions exist but there is little or no impact to the organization's business operations: BCG will provide information or assistance during normal business hours as requested, and where possible. In most cases such assistance will be immediate, but where this is not possible, all efforts will be made to resolve the issue/question within twenty (20) business days.

Changes to the Escalation Procedures are subject to change at BCG's discretion; provided, however, that BCG will not reduce its obligations beyond the level set forth in this Agreement as of the Effective Date.

7.4 Buffalo Computer Graphics Policy/Product Guides. Buffalo Computer Graphics may, in its sole discretion, amend any of its information on its website, including without limitation, its policies and product guides, without notice to Client.

7.5 Technical Issues. Buffalo Computer Graphics may charge back all direct costs to Client associated with an investigation (at the request of Client) relating to a technical issue if Buffalo Computer Graphics concludes that the technical issue is not on its side or is not within the accepted number of support cases (or support window) covered by the Client's Maintenance & Support Package.

7.6 Monitoring. Buffalo Computer Graphics has no obligation to monitor Client's content or use of the Services. However, Client acknowledges and agrees that Buffalo Computer Graphics has the right to monitor content and Client's use electronically from time to time and to disclose any information as necessary to: satisfy any federal, provincial, local or international law, regulation or other governmental request or to do the following:

- a) assist in the pursuit of any legal action, including without limitation, actions against Client;
- b) operate Buffalo Computer Graphics' Services properly; and
- c) protect Buffalo Computer Graphics or its subscribers. Buffalo Computer Graphics reserves the right to either refuse to post or to remove any information or materials from the Services, in whole or in part, that Buffalo Computer Graphics decides, at its sole discretion, is unacceptable, undesirable, or in violation of this Agreement.

7.7 Insurance. Client shall, at its sole cost and expense, procure and maintain in full force and effect throughout the Term or Renewal Term (as applicable), such insurance as is reasonable in Client's industry, including, but not limited to, the following minimum coverages (with Buffalo Computer Graphics as an additional insured):

- a) all risk property insurance on any Client Hardware located at the Facility;

- b) Commercial General Liability insurance for bodily injury, property damage and loss of data in an amount not less than One Million Dollars (\$1,000,000.00) per occurrence;
- c) Workers' Compensation coverage in an amount not less than that prescribed by statutory limits; and
- d) Business Interruption insurance: Immediately upon commencement of the Services and thereafter upon Buffalo Computer Graphics' reasonable request, Client will provide certificates of insurance evidencing such coverage as set forth above. For greater certainty, Buffalo Computer Graphics will not provide insurance coverage for Client Hardware while located at the Facility.

7.8 Supported Browsers/Mobile Devices. Browser support is limited to mainstream browsers (e.g., Google Chrome, Apple Safari, Microsoft Edge, Firefox Mozilla) currently supported by their respective manufacturers (i.e., not deprecated or out of manufacturer support). Support of any browsers that land outside of manufacturer support is subject to additional fees. BCG reserves the right to drop support for any browser at any point during the life of the contract. BCG reserves the right to develop features that will only work in certain browsers even though browsers are covered by manufacturer support.

Browser Mobile support is limited to the latest iteration of the supported mobile platform (iOS and Android). BCG will not extend support to platforms that have been discontinued. Mobile browser support is limited to the primary Browser on the corresponding platform (Chrome on Android and Safari or Chrome on iOS).

8.0 Maintenance Window. Client acknowledges that the Services may be subject to routine maintenance or repair and agrees to cooperate in a timely manner and provide reasonable access and assistance as necessary to allow such maintenance or repair. Scheduled or emergency maintenance terms are identified in the SLA.

9.0 Product Lifecycle. This section refers to both the product as a whole and any modules, features, platforms, and technologies included within or supported by the Software.

9.1 Beta. Beta is defined as the period of time when a new product is tested by Client, but before it is generally available to the market. In preparation for Beta testing, Clients sign up and partner with the BCG development team for field testing. Beta Clients are key partners in validating that the product meets requirements and functions as set out in the product Documentation. During the Beta test period, Clients receive technical support and assistance from the development team.

9.2 General Availability. General Availability occurs when a product successfully completes the Beta period and becomes generally available to the market. This phase begins with a Product Announcement describing the application of the product. Regular releases are planned and full support is offered throughout the General Availability phase.

9.3 Continued Support. Continued Support is the phase a product enters as it approaches its End of Life. From time to time, it is necessary to discontinue a product for a variety of reasons, including lack of market demand, technology obsolescence or the availability of successor products. Once a product enters Continued Support, important milestones are communicated to our Clients throughout the phase. Continued Support for the Product is provided for a minimum of 12 months following the End of Life Announcement. No additional releases of the product are planned during this phase, and Continued Support for a product includes phone and online support. The End of Life Announcement will include an End of Sales date. On this date, the product is no longer available to be licensed, and is removed from the price list. Product support is provided to Clients who purchased a maintenance contract prior to the End of Sales date; maintenance agreements will not extend beyond the End of Life date.

9.4 Retired. Following retirement, support issues may be investigated, at Product Management's sole discretion, in an attempt to provide solutions or workarounds. BCG is under no obligation to provide support for a retired product unless the specific Client's contract expressly states otherwise

10.0 Publicity. BCG may use Client's name as part of a general list of clients. Each Party shall obtain the other Party's permission prior to using the other Party's name for any other marketing or promotional purposes. The Parties agree that any press release or other public comments issued by either Party relating to this Agreement will be prepared jointly between BCG and Client and will be issued upon mutual agreement of the Parties.

[Remainder of this page intentionally left blank]

IN WITNESS WHEREOF the Parties have executed this Agreement as of the date below. (Note: "Effective Date" is defined under the Composition of Agreement on the first page).

BUFFALO COMPUTER GRAPHICS, INC.

CLIENT

Signature

Signature

Name

Name

Title

Title

Date

Date

MASTER SERVICES AGREEMENT (MSA)
Exhibit A – Acceptable Use Policy

The Acceptable Use Policy sets forth the principles, rules, and regulations that govern the use by the Client of Buffalo Computer Graphics' networks, systems, services, and products. This Acceptable Use Policy has been established to promote the integrity, security, reliability, and privacy of Buffalo Computer Graphics' networks, systems, and Client data contained within. BCG may reasonably modify these policies to ensure compliance with applicable laws and regulations and to protect BCG's network and clients. BCG reserves the right to monitor (and suspend if applicable) processes on the (virtual) infrastructure to ensure Client compliance with this Agreement, including the AUP. Such monitoring does not include the monitoring or viewing of any Client Data. If BCG suspends Services for violation of this section, including the AUP, Client remains liable for all fees, charges and any other obligations incurred and accruing. No SLAs credits are payable for any period of suspension.

When using Buffalo Computer Graphics' networks, systems, products, and services the Client is prohibited from engaging in certain activities that include, but are not limited to, those described below. Such prohibited activities may, at the sole discretion of Buffalo Computer Graphics, be grounds for termination of Agreement with a Client, for the application of additional service charges or for the involvement of law enforcement agencies. Buffalo Computer Graphics reserves the right to remove any content or restrict the use of the Services for activities or content that in Buffalo Computer Graphics' reasonable judgment, violate the terms or conditions under which Buffalo Computer Graphics provides the Services or violate this Policy.

Indirect or attempted violations of the policy, and actual or attempted violations by a third party on behalf of a Buffalo Computer Graphics Client or a Client's end user, shall be considered violations of the policy by such Client. Buffalo Computer Graphics reserves the right to change the Policy by delivering notice of its decision to change the Policy to the Client at least 15 days prior to the changes taking effect. If you have any questions about this Policy, please contact Buffalo Computer Graphics at info@bcgeng.com.

Prohibited Uses of Buffalo Computer Graphics' Services and Products

This section of the Acceptable Use Policy identifies the uses and actions that Buffalo Computer Graphics considers in its reasonable judgment to be unacceptable and/or abusive, and thus, is strictly prohibited. The Client may only use Buffalo Computer Graphics' networks, systems, services and products in a manner that, in Buffalo Computer Graphics' sole judgment, is consistent with the purposes of such networks, systems, services and products. The following examples of prohibited uses and actions are non-exclusive and are provided for general guidance only.

1. to violate any law of any applicable jurisdiction, including, without limitation, laws governing advertising, alcohol, antitrust, child protection, drugs, encryption, exportation, food, financial services, firearms, gambling, importation, information systems, intellectual property, obscenity, privacy, securities, telecommunications and tobacco;
2. to commit a tortious or otherwise wrongful act, including, without limitation, the posting or communication of libelous, defamatory, scandalous, threatening, harassing, or private information without the permission of the person(s) involved, or posting content that is likely to cause emotional distress, whether through content, frequency, or size;
3. to engage in or to facilitate gambling activities;
4. to post, send, or receive any content that is obscene, pornographic, lewd, lascivious, or excessively violent;
5. to offer, solicit, sell, buy, rent, or license any goods, products, services, or information in, from, or to any location in which such activity is unlawful;
6. to advocate, promote, or otherwise encourage violence against any government, organization, group, individual or property, or to provide instruction, information, or assistance in causing or carrying out such violence;
7. to post, send, receive, display, distribute, or execute any content, including, without limitation, text, graphics, images, music, recordings, computer programs, links, frames, and "meta tags," that violates any copyright, right of publicity, patent, trademark, service mark, trade name, mask work, trade secret or other intellectual property right of others or use any tools designed to facilitate such access, such as packet "sniffers";
8. to delete or alter author attributions, copyright notices, or trademark notices, unless expressly permitted in writing by the owner;
9. to violate the terms of applicable software licensing agreements;
10. to obtain or attempt to obtain unauthorized access, such as attempting to circumvent or circumventing any authentication or other security feature of any system, network, or account. This includes accessing data not intended for the user, logging into a server or account the user is not authorized to access, or probing the security of any system, network, or account;
11. to interfere or attempt to interfere with service to any user, host, or network by use of any program, script, command, or otherwise. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service or to burden excessively a service's resources, and attempts to "crash" a host;
12. to introduce worms, harmful code and/or Trojan horses;
13. to attempt to circumvent the approval process for posting to a moderated newsgroup or bulletin board or to attempt to evade spam filters;
14. to cancel or supersede posts other than your own, with the exception of official newsgroup or bulletin board moderators performing their duties;
15. to send or post unsolicited messages or e-mail, whether commercial or not,
 - a) to any recipients who have requested that messages not be sent to them, or
 - b) to a large number of recipients, including users, newsgroups, or bulletin boards, at one time; or to collect responses from unsolicited email sent through the Services or from other external systems;
16. to send or post a message whose subject or content is unrelated to the subject matter of the newsgroup or bulletin board to which it is posted;
17. to send or post a message or e-mail with deceptive, absent, or forged header or sender identification information;
18. to propagate chain letters and pyramid schemes, whether or not the recipient wishes to receive such mailings;
19. to use Internet Relay Chat "bots";
20. to hold Buffalo Computer Graphics, its affiliates, officers, employees and/or shareholders up to public scorn or ridicule;
21. to resell Buffalo Computer Graphics' services, in whole or in part, to any entity or individual, without Buffalo Computer Graphics' prior written consent, or to misrepresent your relationship with Buffalo Computer Graphics
22. to forge, alter or remove header information or Client's identity;
23. to exceed any bandwidth caps or other limitations imposed by any of Buffalo Computer Graphics' underlying service providers;
24. to use the Internet in a manner that is not authorized by Buffalo Computer Graphics or its underlying service providers;
25. to operate a server in connection with Buffalo Computer Graphics or the Services for purposes other than for Client's normal business activity, including but not limited to mail, news, file, gopher, telnet, chat, web, or host configuration servers, multimedia streamers, or multi-user interactive forums; and/or
26. to use Buffalo Computer Graphics or the Services for operation of an ISP's business or for any other business enterprise in competition with Buffalo Computer Graphics.

Client is responsible for any misuse of the Services that it contracted for under this Agreement, even if the misuse was caused by its employee(s), contractor(s) or other third party(s) that had access to the Services. Client is responsible for ensuring that others do not gain unauthorized access to the Services. Client is solely responsible for obtaining, installing and maintaining all Client provided equipment and related services necessary to connect to Buffalo Computer Graphics' network. Client shall not connect or interconnect its equipment with any other equipment or services of any third party without Buffalo Computer Graphics' prior written consent and such consent shall not be unreasonably delayed or withheld. Client is solely responsible for the security of any device that Client connects to the Services, including any data stored on that device. In addition to Buffalo Computer Graphics' termination rights as set out in the Agreement, the Client engaging in one or more of these activities may result in, at the sole discretion of Buffalo Computer Graphics, acting reasonably, the suspension of Services (in whole or in part). Buffalo Computer Graphics may pursue any remedies available to it under the Agreement in the event of Client's breach of this AUP.

MASTER SERVICES AGREEMENT (MSA)

Exhibit B – Client Information Form

CLIENT CONTACT INFORMATION			
Legal Entity Name:			
Address:			
City:			
Province:		Postal code:	
Main Telephone:		Main Facsimile:	
HST#		PST Number?	
Email for notices:			
Email for invoicing:			

PRIMARY CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

BILLING CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

TECHNICAL CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

MASTER SERVICE AGREEMENT (MSA)

Exhibit C - BCG Managed Services Order Form/Statement of Work (SOW)

Quote Number:	
Project Manager / CSR:	
Client:	
Client Contact / PM (name):	
Client Contact (email):	
Client Contact (phone):	
Term:	
Term Start Date:	
Initial Term End Date:	
Annual Fee (excluding taxes):	
Onetime Fee (excluding taxes):	
Payment Terms:	
Billing Commencement Date:	
Services to be Provided:	
Client Responsibilities:	
Notes:	
Hosting Requirements:	
Hosting Data Center/Location:	
Terms & Conditions:	

BCG Signature

Client's Signature

Title

Title

Date

Date

MASTER SERVICES AGREEMENT (MSA)

Exhibit D – BCG Service Level Agreement

Updated 9/1/2020

This SLA is provided pursuant to and in accordance with the governing service agreement between Client and Buffalo Computer Graphics, Inc. The following Service Level Agreement (SLA) is applicable to the BCG Cloud Services Client for a fee and all credits are offered due to uptime guarantee failures. The SLA is not applicable to unrelated third parties or third parties lacking a contractual relationship with BCG. The uptime obligations and the resulting SLA credits are applied on a monthly basis unless specified otherwise in Exhibit E.

Public Network: BCG will deliver 99.9% uptime availability on all Public Network services to Clients located in BCG’s Partner Cloud data centers. All Public Network services include redundant carrier grade Internet backbone connections, advanced intrusion detection systems, and denial of service (DOS) mitigation. This does not include DOS attacks or other unknown variables that can affect Internet traffic and are excluded from the issuance of SLA credits.

DisasterLAN (DLAN) Application: BCG will deliver 99.9% uptime availability on the DLAN Application. A DLAN Application failure occurs when a Client cannot access the DLAN Application because of problems with hardware and/or software in BCG’s control. Access issues caused by problems connecting to the service, including without limitation problems on the Internet or access and configurations managed by a non-BCG provider, do not constitute failures and as such are not covered by this SLA. Clients will receive a service credit for the period of time commencing when a ticket is filed requesting assistance in accessing the DLAN Application and the access issue is verified by BCG until the services are reinstated.

Third Party Applications: BCG Cloud Services utilize a number of third-party services that are used to enhance content within BCG’s base product including but not limited to AERIS weather, ESRI ArcGIS Online services, Microsoft Bing Services, and Google Map Services. These third-party services are not covered by BCG uptime availability guarantees and are out of BCG’s control. While downtime related to these services will not affect BCG products directly in terms of overall functionality, it could result in these enhanced content offerings being unavailable at a time of need. Access issues related to these third-party applications do not constitute failures and are not covered by this SLA. Additionally, BCG makes no guarantees about the content or availability of services made available in BCG products via these third parties. Third party services are subject to the licensing terms of these said third parties and services offerings made by said third parties may be changed by the third party at any time. The modification, addition, or removal service offering from said third parties shall not constitute a breach in this SLA or any other agreement with BCG. Should said third parties make a change that may impact offerings available to the customer, BCG will notify the customer about such changes and offer alternative solutions if available. BCG will work in good faith to resolve any issues with third-party-provided data and services including the option to provide alternate data/service providers if necessary.

Simple Backup Service: BCG will perform nightly backups of application code and data and retain backups for 7 days.

Simple Disaster Recovery Service: BCG will provide an RPO time of 24 hours and an RTO time of 72 hours.

Maintenance: At certain times planned maintenance is required on the BCG Cloud that can cause service disruption. Maintenance services can affect the Public Network, Private Network, Virtual Servers, Cloud Storage, Security and other services. BCG will notify Client of planned maintenance service. BCG will provide at least 24-hour notice to Clients for potentially disruptive maintenance activity via email.

"Emergency Maintenance" refers to any corrective action intended to remedy conditions likely to cause severe Service degradation or correct critical security impacts, as designated by BCG in its sole discretion. Emergency Maintenance may include but is not limited to actions intended to address hardware or software failures or viruses/worms. BCG will exercise reasonable efforts to inform Client in advance before interrupting the Service for Emergency Maintenance, but such notice is not guaranteed and failure thereof does not constitute failure.

Support Response Time:

Note: The support details described in this section are applicable to BCG Cloud Services including the DLAN Application. BCG’s standard business-day hours are 9 AM – 5 PM Monday-Friday (excluding holidays) Eastern Time. Clients can submit service-related issues at times in accordance with the terms of their contracted support tier (e.g., business day, 24/7/365).

Problem	Severity	Impact	Description and Resolution Support
---------	----------	--------	------------------------------------

Severity	Code		Requirement
1	Critical	Mission Critical	System is not operational/unavailable/significant measurable performance degradation: BCG will commit a full-time resource, or team of resources, to resolve the problem as soon as possible. All efforts will be made to resolve the issue within a twenty-four (24) hour period.
2	High	Major	Critical functionality is not operational: BCG will commit a full-time resource, or team of resources, during normal business hours to resolve the issue as soon as possible. All efforts will be made to resolve the issue with a forty-eight (48) hour period.
3	Medium	Moderate	Non-critical functionality is not operational: BCG will commit a resource, or team of resources, during normal business hours to restore service to a satisfactory level. All efforts will be made to resolve the issue within five (5) business days with either a fix or suitable workaround.
4	Low	Minor	Specific issue or questions exist but there is little or no impact to the organization's business operations: BCG will provide information or assistance during normal business hours as requested, and where possible. In most cases such assistance will be immediate, but where this is not possible, all efforts will be made to resolve the issue/question with either a fix or suitable workaround within twenty (20) business days.

Critical: Severity 1 Tickets receive a 30 minute time-to-acknowledge.

High: Severity 2 Tickets receive a 60 minute time-to-acknowledge.

Medium: Severity 3 Tickets receive a 1 business day time-to-acknowledge.

Low: Severity 4 Tickets receive a 1 business day time-to-acknowledge.

For all issues, Client must contact BCG support [via email at dlansupport@bcgeng.com or via phone] and create a ticket for which a tracking number will be provided and a support engineer assigned to review the support request within the timeframe listed above. If for some reason Client does not receive a response within the prescribed time intervals, Client should contact client care by phone and request that the support response be expedited.

BCG may reclassify any Ticket misclassified as falling into one of the Critical or High Priority categories listed above and such Ticket will not qualify for Critical or High Priority treatment.

Incident Reports: BCG will provide Client with an Incident Report via e-mail within seventy-two (72) hours for incidents resulting in greater than thirty (30) minutes of downtime. The Incident Report will include: incident date, duration, issue, details of the problem and details of the resolution.

SLA Credit Claim:

If a Client believes that a service failure occurred which occurs when the services are not available in accordance with this Agreement occurred, Client must open a support ticket (a "Ticket") by contacting BCG Support by email to dlansupport@bcgeng.com or via phone, and request any credits by accurately detailing the credit request within 30 days of the failure in question. BCG will issue to the Client appropriate service credits for the failure as defined in this SLA upon review and confirmation of the service failure.

Credit Limitations:

- 1) The minimum period of failure eligible for a credit is 15 consecutive minutes, and shorter periods will not be aggregated. The maximum credit shall not exceed one hundred percent (100%) of Client's fees for the affected Service feature for the then-current billing month. In the event that multiple periods of failure overlap in time, credits will not be aggregated, and Client will receive credit only for the longest such period of failure. In the event that a single incident calls for credits pursuant to multiple parts of this SLA, BCG will award credits for all Service features impacted in a single incident subject to the maximum credit noted above.

- 2) Credits available pursuant to this SLA will apply to future service delivery and will be credited against the applicable invoices. In the case where there will be no further invoices, BCG will pay the amount of the service credits to Client in cash, by check or wire transfer, within 60 days after the end of the Agreement.
- 3) Notwithstanding any provision to the contrary in this SLA, the following do not constitute failures:
 - a. downtime during planned maintenance (as defined above) or Emergency Maintenance (as defined below) periods;
 - b. outages caused by acts or omissions of Client that are prohibited by this Agreement;
 - c. outages caused by hackers, sabotage, viruses, worms or other third party wrongful actions if not detected by BCG's intrusion detection;
 - d. DNS issues outside of BCG's control;
 - e. outages resulting from Internet anomalies outside of BCG's control;
 - f. outages resulting from fires, explosions, or force majeure;
 - g. failures during a "beta" period;
 - h. any permissible suspension of Service pursuant to the Agreement;
 - i. during a time in which a Client is not in compliance with the AUP; or
 - j. the unavailability of required Client personnel, including as a result of failure to provide us with accurate, current contact information.

Exclusions:

- 1) This SLA provides Client's sole and exclusive remedies for any breach of the Service Levels set forth in this SLA.
- 2) This SLA does not cover (without limitation): (a) network performance to Client's physical location or Internet access point (such as a local DSL/cable modem); or (b) internal network issues or failures; or (c) failures due to denial of service attacks.
- 3) False or repetitive claims are subject to service suspension. Clients participating in malicious or aggressive Internet activities, thereby causing attacks or counter-attacks, do not qualify for SLA claims and shall be deemed in violation of the Acceptable Use Policy posted on the Website.
- 4) This SLA covers production-level servers and services, and does not apply to beta, sandbox, test, evaluation, training, or demo servers and services.

Credit Issued: For all SLAs, the service credit formula is as follows:

Hours of eligible downtime due to failure x Product and/or Service hourly cost = service credit.

- Credit Eligible Downtime due to failure = Time (in hours) past the SLA greater than 15 minutes excluding allowable downtime
- Product and/or Service hourly cost = Client's billing rate/hour during period of downtime of failure

MASTER SERVICE AGREEMENT (MSA)

Exhibit E – MSA/SLA Amendments

Revised 9/1/2020

The following outlined changes/additions to the BCG Master Services Agreement and/or SLA have been agreed upon by both BCG and the Client and supersede the corresponding respective Terms and Conditions outlined in the standard baseline MSA/SLA. Customer pricing shall reflect any additional fees necessary to provide the outlined changes/additions/upgrades.

- 1) **Hosting/Server Location(s)** – BCG will host the DLAN application and all respective data at one of our enterprise-class North American data centers provided by our hosting partner TBD.
- 2) **Concurrent Users** – System shall be architected and configured to support TBD concurrent users.

BCG Signature

Title

Date

Client's Signature

Title

Date



Emergency Management Information System

WV DHS Emergency Management Division

CRFQ 0606 HSE2200000005

Due 12/21/2021

Prepared for:

David H. Pauline

Dept. of Administration, Purchasing
Division

2019 Washington St E

(304) 558-0067

david.h.pauline@wv.gov

Prepared by:

Patrick Cerra

Buffalo Computer Graphics, Inc.

4185 Bayview Road

Blasdell, NY 14219-2732

716-822-8668

rfpteam@bcgeng.com

CONTENTS

- SOLICITATION DOCUMENT 5
- ADDENDUMS 7
- EXECUTIVE SUMMARY 8
- 3. QUALIFICATIONS 10
- 4. GENERAL REQUIREMENTS 19
- 11. MISCELLANEOUS 88
 - 11.1 Contract Manager 88
 - 11.2 Software as a Service Addendum 88
- APPENDIX A 99

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: BUFFALO COMPUTER GRAPHICS, Inc.

Name of Agency: West Virginia Emergency Management Division

Agency/public jurisdiction's required information:

- 1. Will restricted information be processed by the service provider?
Yes
No
- 2. If yes to #1, does the restricted information include personal data?
Yes
No
- 3. If yes to #1, does the restricted information include non-public data?
Yes
No
- 4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes
No

5. Provide name and email address for the Department privacy officer:

Name: PATRICK LUPIANI
Email address: PLUPIANI@bcgeng.com

Vendor/Service Provider's required information:

- 6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:
Name: PATRICK LUPIANI
Email address: PLUPIANI@bcgeng.com
Phone Number: 716 822 8668

..... 99

EXHIBIT A – PRICING 100

SIGNED PURCHASING AFFIDAVIT 101

SAMPLE BCG MASTER SERVICES AGREEMENT 103



SOLICITATION DOCUMENT



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Quote

Proc Folder: 970413			Reason for Modification:
Doc Description: Emergency Management Information System (EMIS)			
Proc Type: Central Contract - Fixed Amt			
Date Issued	Solicitation Closes	Solicitation No	Version
2021-11-24	2021-12-14 13:30	CRFQ 0606 HSE2200000005	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code: VS0000016546
Vendor Name: BUFFALO Computer Graphics, Inc.
Address: 4185 Bayview Road
Street:
City: BLASDELL
State: NY **Country:** US **Zip:** 14219
Principal Contact: Patrick CERRA
Vendor Contact Phone: 716 822 8668 **Extension:** 103

FOR INFORMATION CONTACT THE BUYER

David H Pauline
 304-558-0067
 david.h.pauline@wv.gov

Vendor Signature X *Gay D. Masterson* **FEIN#** 161190997 **DATE** 3-Dec-2021

All offers subject to all terms and conditions contained in this solicitation

ADDENDUMS

Signed addendums list

ADDENDUM ACKNOWLEDGEMENT FORM SOLICITATION NO.:

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | | | |
|-------------------------------------|----------------|--------------------------|-----------------|
| <input checked="" type="checkbox"/> | Addendum No. 1 | <input type="checkbox"/> | Addendum No. 6 |
| <input checked="" type="checkbox"/> | Addendum No. 2 | <input type="checkbox"/> | Addendum No. 7 |
| <input type="checkbox"/> | Addendum No. 3 | <input type="checkbox"/> | Addendum No. 8 |
| <input type="checkbox"/> | Addendum No. 4 | <input type="checkbox"/> | Addendum No. 9 |
| <input type="checkbox"/> | Addendum No. 5 | <input type="checkbox"/> | Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Buffalo Computer Graphics, Inc
Company

David Masterson
Authorized Signature

3-Dec-2021
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

EXECUTIVE SUMMARY

RFP Subject: Emergency Management Information System

Number: CRFQ 0606 HSE2200000005

Vendor's Name: Buffalo Computer Graphics, Inc.

Business Address: 4185 Bayview Road, Blasdell, NY 14219

Phone: 716-822-8668

Fax: 716-822-2730

Contact: Patrick Cerra

Email: rfpteam@bcgeng.com

Buffalo Computer Graphics, Inc. (BCG) appreciates the opportunity to respond to West Virginia Emergency Management Division's (VWEMD) request for proposal for a web-based statewide EMIS enterprise solution.

BCG is privileged to have provided emergency management focused software solutions for American and Canadian governments and private entities for nineteen years, and maritime training, simulation, and communication software and hardware for thirty-nine years. We are experts with the requirements and technology landscape of emergency management agencies and departments and believe that we can provide a tailored configurable-off-the-shelf software solution that meets and exceeds the needs of VWEMD and its stakeholders involved with the State's EMIS platform.

BCG's proposal includes a configurable software solution based on its COTS DisasterLAN (DLAN) emergency management information system cloud-based software platform that can serve as a central emergency response platform and EMIS software system with scalable state-wide coverage. This solution will accommodate all VWEMD's projected users including VWEMD System Administrators, State Agency Representatives, Local Jurisdiction Representatives, Non-Governmental Organizations, Federal Agency Representatives, and other EMIS participants in terms of both scalability and feature sets designed for multi-agency collaboration. The DLAN system facilitates both day-to-day and emergency incidents by providing a modern web-based software solution with mobile applications.

BCG's DLAN products have already been successfully implemented for multiple State Agencies in the USA and Provincial Agencies in Canada. As a current example, BCG implemented a solution for the State of Oregon Department of Human Services in 2021 with an expedited timeframe. The success of this project has already led to an additional expansion to expand the solution with additional products and services for sheltering and refugee services management. In BCG's home state of New York, the New York State Department of Homeland Security & Emergency Service currently uses BCG's software as part of their NY-Responds statewide emergency management system, which can be accessed by all 62 New York State Counties as part of the State-wide implementation. The DLAN system is also utilized by all NYS Functional Groups, State Agencies, New York State Division of Military and Naval Affairs (National Guard), and many other stakeholders and organizations. BCG believes a similar model and implementation methodology would be successful for the State of West Virginia.

As a well-established provider of EMIS systems, BCG can provide a smooth fast implementation process to get customers up and running quickly. To achieve this end, BCG will work with Infinite One Technology Solutions, a long-time support partner who provides project oversight, coordination, and implementation services. BCG the

prime vendor. BCG agrees that it is able to implement the software within four months of final contract signing as per Addendum #2's additional mandatory requirement.

BCG is a company that is committed to excellence in emergency and incident management. The company requires that all employees that work on DLAN train in FEMA's ICS courses. Additionally, BCG's core management and many engineer staff come from emergency management or firefighting backgrounds. BCG can provide trained ICS staff and IMAT teams to supplement VWEMD's EMIS during a response. BCG understands the Emergency Operation Center environment, field response, planning, and executive decision making better than other software vendors, because we are emergency managers ourselves. This knowledge shines through in DLAN's thoughtful design, its ability to digitize key processes, and its multi-agency ready feature set. The system allows users to not just capture information for situational awareness and accountability, but to operationalize it in a meaningful way for effective decision making, prioritization, and task completion.

Thank you for the opportunity to present our DLAN system in our response to this RFP which we believe will successfully address VWEMD's mission to support statewide use by state agencies, local governments, regional and national partners, and private response partners throughout both day-to-day use and all areas of homeland security and emergency management.

Sincerely,



Patrick J. Cerra
Proposal Manager, BCG
22 December 2021

3. QUALIFICATIONS

Vendor, or Vendor’s staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1 Vendor shall provide a minimum of five (5) relevant reference to demonstrate that it has proven experience in managing hosted/on-premises Solutions at a statewide level. All referenced Solutions shall be currently operational in a production environment. This information shall be provided prior to contract award.

Reference #1 Oregon Department of Human Services

Oregon Department of Human Services (ODHS) – Emergency Management			
Contact Person:	Steve Pegram, Executive Director		
Contact’s Email:	Steve.s.pegram@dhsosha.state.or.us		
Address:	500 Summer St NE, E-15, Salem, OR 97301		
Contact’s Phone:	503-366-3934	Date of Service:	8/17/21-Present
Modules:	This is a DLAN Premium system with the following modules: Bed Tracking, Finance, GIS Premium, HICS Forms & Job Action Sheets, Special Needs Module, Chat, Communication Center, GIS, Incident Folders, Mobile Responder, Phonebook, Phonebook Premium, Reference Library, Resource Database, Social Media Basic, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Healthcare Industry Pack, ICS or IMS Forms Module, Incident Action Plan Module, Role Checklist Module, Situation Report Module, Damage Assessment Form, Report, & Board, Road Closure Form, Report, & Board, Role/Task Status Report & Board, Shelter Management Form, Report, & Board, and the Sheltering Module		
Scope of Work:	<p>Summary: This is a BCG cloud hosted 4-year contract. The system includes the DLAN Premium Edition with the Emergency Management Pack, Healthcare Pack, Finance Module & GIS Premium. The Oregon Department of Human Services (ODHS) is a state-wide agency with purview daily citizen services and programs as well as long-term risks and impacts from emergency and public health events. ODHS particularly focuses on critical human services such as short-term housing, sheltering, COVID-19 assistance, and supporting vulnerable populations.</p> <p>Details: In 2020 the State of Oregon recognized that short term and long-term impacts from the global pandemic required additional support and services from the State. A new emergency management team was created under the Department of Human Services to address coordination, planning, awareness, and services to Oregonians impacted by emergencies.</p> <p>ODHS implemented the DLAN software system in an expedited time frame. ODHS and BCG worked to design and deploy a system of dashboards based on FEMA’s Lifelines. This capability has allowed ODHS to collect situational information updates and essential</p>		

	elements of information from teams, departments, and facilities across the state. In addition to lifelines, ODHS and BCG implemented significant shelter staff management tools using the DLAN Mobile Responder App. A substantial expansion to ODHS' sheltering is planned for early 2022 focusing on family reunification, staff tracking, and other elements of long term sheltering.
--	--

Reference #2 Province of Ontario, Office of the Fire Marshal and Emergency (OFMEM)

Ontario Office of the Fire Marshal and Emergency Management (OFMEM)			
Contact Person:	Danylo Zakydalsky, Emergency Management Operations Officer		
Contact's Email:	Danylo.zakydalsky@ontario.ca		
Address:	Ontario Office of the Fire Marshal and Emergency Management (OFMEM) 25 Morton Shulman Ave, 5th Floor ,Toronto, Ontario M3M 0B1 Canada		
Contact's Phone:	647-329-1062	Date of Service:	2019 - Present
Modules:	This is a custom designed DLAN system. Modules include: Asset Management, Chat, Communication Center, finance Module, GIS Premium, IAPs, Incident Folders, Mobile Responder, Phonebook, Reference Library, Resource database, Situation Reports, Social Media Premium, Status Board Builder, Ticket Manager Premium, Additional Training Site.		
Scope of Work:	<p>Summary: DLAN enables the Province of Ontario to improve the input of necessary information to better support the monitoring, oversight, response and recovery to incidents that occur in vast Ontario communities and within the Ontario Public Service (OPS) organization. After a rigorous procurement process, Buffalo Computer Graphics (DLAN software) was selected by the Province.</p> <p>The DLAN software greatly enhances overall Provincial situational awareness during incidents, facilitates resource requests between stakeholders, assists in debris management and disaster assessments and streamlines emergency communications. Access to the system, which is also available on mobile devices, is being provided to emergency management officials within numerous provincial ministries, federal departments, municipalities, First Nations communities and select industry partners.</p> <p>Details: The robust DLAN software solution they have chosen supports all aspects of the Ontario Incident Management System (IMS). IMS serves as a framework in DLAN that guides organizational structures, functions, processes, and terminology. In addition to this, DLAN also includes standardized IMS values, forms, and fields in all areas of the system. DLAN exceeds other software solutions by taking these aspects and standardized values from IMS and using them to build out supportive processes, workflows, and response modules that work hand in hand to support technical and functional interoperability for both planned and unplanned events in Ontario.</p> <p>DLAN encourages an IMS based process for Ontario's handling information in the system at the following levels:</p> <p><i>User Level:</i> Each end-user has a clearly defined role/position in DLAN and receives tickets and messages tasked to his or her specific role that need to be managed or acknowledged. Role specific dashboards, homepages, and reports make information management and</p>		

	<p>interacting with the system quick and simple. Users pass information along to the next relevant role or person in the chain and all interactions are automatically logged. This helps maintain span of control and accountability for upper management.</p> <p><i>Section Level:</i> DLAN supports Ontario’s Dynamic Organizational Structures based on IMS standards. Each active IMS section (ex: Logistics, Operations, Planning, Fin/Admin, and Command) has access to specific software features designed to assist that section in performing their duties in response to the incident or event.</p> <p><i>Command Level:</i> Standardized and completely customizable reports in DLAN are available to command staff so that they can make timely decisions based on current information. For example, an Incident Commander or Executive dashboard may incorporate a ticket report showing life safety issues, a critical decisions list, an annotated GIS map of the incident area and affected infrastructure, and a curated social media stream of reliable source information.</p> <p><i>Multi-Agency and Multi-Jurisdictional Coordination Level:</i> DLAN supports Ontario’s coordinated communication and information sharing via standardized methods such as the ability to Email or forward documents and content out from the DLAN system to designated partners and other jurisdictions.</p> <p>For the ultimate coordination of Ontario’s emergency information, DLAN’s Ticket Sync feature allows real-time data synchronization between entities using their own DLAN software system in the region. OFMEM can directly exchange data with the City of Toronto OEM, City of Mississauga OEM, Halton Regional EOC, Toronto Hydro ESL, EMCT (Ontario Ministry of Health MOHLTC and LHINS), and neighboring cross-border entities such as New York State and Erie County, NY. OFMEM has the ability to send and receive critical information reports and resource requests including the ability to see comments and updates from ticket sync partners in real-time further enhancing a regional approach to incident management.</p>
--	--

Reference #3 NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)

New York State Department of Homeland Security and Emergency Management			
Contact Person:	David Smith, Operations Section Chief		
Contact’s Email:	david.smith3@dhSES.ny.gov		
Address:	NYS Office of Homeland Security & Emergency Management 1220 Washington Avenue State Office Campus Building 22 Albany, NY 12242 United States		
Contact’s Phone:	518-292-5955	Date of Service:	2004 - Present
Modules:	This is a DLAN Premium system. Modules include: Chat, Communication Center, GIS Basic, Incident Folders, Mobile Responder, Phone Book, Phonebook Premium, Reference Library, Resource Database, Social Media, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Emergency Management Industry Pack,		

	ICS, IAP, Role Check list, Situation Reports, Damage Assessment, Weather, Separate Training Site, Watch Command
Scope of Work:	<p>Summary: The State of New York has branded their uniquely configured DLAN system as “New York Responds” for use within their State. They employ a full featured On Premise DLAN Enterprise solution with the addition of Ticket Manager Premium, Role Activity Log, Watch Command, Asset Tracking, Chat, GIS Premium, Training Site, and Watch Command Modules. Renamed as NY-Responds for the state of NY, the system is designed to be used by any county or state agency throughout NYS.</p> <p>Three days prior to the start of the Republican National Convention (RNC) in Madison Square Garden New York City, the director of DHSES called BCG with a statement that DHSES’s home-brewed EMIS had failed and that they had chosen DLAN from among 20 other systems as its replacement. They needed DLAN installed and running immediately. To meet this request, BCG staff travelled to DHSES, installed the system overnight, and spent Sunday testing and training core staff. Just-in-time training was provided to end-users and the system was used successfully throughout the RNC with people logged in from Albany, NY, New York City, Madison Square Garden event center, and New Jersey to manage the event. Over the long duration of its use at the NYS’s DHSES state-level emergency operations center, DLAN has transitioned from an early Version 3.1 to the current Version 12.x and has adapted to meet the mission critical resource requesting and tracking needs for NYS. Ongoing development work for DHSES over the years has helped BCG staff develop the skills necessary to design, build, and implement systems suited for statewide, multi-jurisdictional needs and deliver them on time and within budget. Recently, NYS has re-implemented the NY Responds system, of which BCG software is a key component. This unique statewide system allows all 62 counties to utilize one unified, feature-rich incident management solution. BCG has worked closely with the State to ensure the success of this ambitious project.</p> <p>Details: New York State has an extended support and maintenance package with BCG. In addition to our typical Platinum Plus Support plan, DHSES has added dedicated blocks of time to support their agency in a number of ways during daily usage, training, exercises, and EOC activations. Since BCG is intimately involved in the State’s workflows and procedures, the agency has also elected to have stand by contracting in place for onsite work that can be leveraged during trainings, exercises, and EOC activations in order to ensure that they have the vendor support they need to provide services like just-in-time training, workflow training specific to a user’s role, new feature training as upgrades come out, and support for onsite meetings for proposed features. In addition, the State has such confidence in BCG staff that they elected to include hours for BCG to support them in diagnosing non-DLAN issues such as client, server, and network problems that may impact their users. With BCG actively involved onsite in EOC activities, our staff is often able to diagnose an issue more quickly than external IT staff, allowing their staff to relay issues to IT more efficiently. Finally, in large activations like Hurricanes Irene and Sandy, the State has contracted with BCG to provide around-the clock 24/7 support within the EOC to assist them with both on-site troubleshooting and training during these large activations.</p>

Reference #4 New York Power Authority (NYPA)

New York Power Authority (NYPA)

Contact Person:	Joseph Flick, Director of Emergency Management		
Contact's Email:	joseph.flick@NYPA.gov		
Address:	123 Main Street, Mail Stop 10- H, White Plains, NY 10601		
Contact's Phone:	914-390-8095	Date of Service:	2017-Present
Modules:	DLAN Advanced with: GIS Premium, Phonebook Premium, Role Activity Log, Situation Reports, Status Board Builder, Ticket Manager Premium, Training Site, Weather		
Scope of Work:	<p>Summary: Although the original DLAN system was installed for NYPA in 2017, their use of the multi-featured software continues to grow and evolve to meet the changing needs of the organization. In addition to ramping up to meet any emergency situations that arise, the system is used in a day to day capacity to send and monitor Incident Notifications and to provide Situational Awareness from inside the control rooms. Ensuring 24/7 capabilities on a day-to-day operation, their staff uses the system to manage any individual incident that requires documentation and follow up, and also provides them with the capability to send notifications to other team members around the state.</p> <p>Details: DLAN provides the support the Power Authority needs to manage their critical business. For example, the DLAN system was able to immediately send Incident notifications to their predefined list of members that needed to be notified of a specific situation. In a matter of seconds – an operator (via PC or mobile device) could automatically generate a notification to particular staff across the state. The ability to provide information at a moment's notice is essential to their operation. As a web-based tool, DLAN allows offsite staff to quickly log in and provide status and information to the location at headquarters.</p> <p>A seamless transition has been provided to the Power Authority as this organization has transitioned from a deprecated, silo-ed system to DLAN. This allows the control rooms onsite and offsite staff to efficiently and easily participate at any time, and eliminates duplication of efforts as they manage their daily or emergency affairs. As situational awareness tool, NYPA utilizes DLAN to manage daily events and keep track of a variety of information that affects their state-wide operation. Utilizing the GIS mapping tools and Status Boards, information can quickly and efficiently be shared.</p> <p>This client also employs a totally separate Training Site. This allows users to have training any time on a DLAN system set up exactly like the live site. In addition the training site can be used for exercise play without the need to worry about interfering with daily operations.</p>		

Reference #5 LAMACS System - City of El Segundo California

LAMACS-City of El Segundo, California, Emergency Management/Disaster Preparedness			
Contact Person:	Randal Collins, Emergency Management Coordinator		
Contact's Email:	rcollins@ahimta.org		
Address:	LAMACS - City of El Segundo California 350 Main St., El Segundo, CA 90245		
Contact's Phone:	(310) 524-2366	Date of Service:	2021 - Present
Modules:	DLAN Advanced with: Asset Tracking, Mobile Responder, Emergency Management Pack, Chat, GIS Premium, Phonebook Premium, Status Board Builder, Streaming		

	Video, Ticket Manager Premium, Reference Library, Resource Database, Status Board, Reference Library, Training site.
Project Description	<p>Summary: Buffalo Computer Graphics was recently selected to provide DisasterLAN incident management software to the 88 cities within the Los Angeles Operational Area. In late 2020, the cities within the LA Operational Area worked together to procure emergency management software for the region. The project was spearheaded by Randal Collins, the City of El Segundo Emergency Management Coordinator. He, along with fellow colleagues, saw the need for a coordinated, integrated common operation picture that spanned the entire County and connected all the emergency managers and other stakeholders onto one platform.</p> <p>BCG provided a DLAN Advanced system that would provide elected officials, city managers, department directors, operational managers, and other partners with situational awareness of incidents and events. The system allows all of the municipalities to manage situations within their jurisdictions and also to coordinate with each other on multi-jurisdictional emergencies. They also chose to utilize BCG’s Platinum level of maintenance to afford them the highest level of support coverage. BCG provides a hosted solution for 500-1000 users, and the system continues to expand as they add additional areas and organizations. Because of their rapid and ongoing expansion to additional organizations, training has been a huge part of the installation.</p> <p>Details: After a competitive RFP process, BCG’s DLAN software was selected. One of the main reasons DLAN was chosen is that the system does not include individual user licenses. This means that various partners across municipalities could be added to one system quickly and easily. The intuitive user interface meant new users need minimal training to effectively use the system. This makes it easy to bring in additional parties during a crisis. This customer chose to add a premium level of GIS to enhance their system mapping capabilities, along with Ticket Manager Premium and the Incident Action Plan Module.</p> <p>The Los Angeles Operational Area liked DLAN’s flexible and modular design that allowed them to add on features as needed. DLAN’s system is also fully configurable, so the system was setup to fully meet the exact needs of this critical area in California. Collins notes “You don’t get that level of customization with other products.” He also remarked that the in-depth implementation process really helped the cities work through the various processes and workflows necessary to make a cross jurisdictional system work for all involved. Collins commended the BCG team on their responsiveness throughout the process and even noted that the team proactively pushed the project forward.</p> <p>“BCG really took the reins and guided us through the entire process. They were relentless in scheduling meetings and making sure forward progress kept happening... BCG’s commitment to project management really took the burden off of the emergency management staff and saved them a lot of time.” Randal Collins – City of El Segundo</p> <p>The City of El Segundo is utilizing the system for their own daily and emergency operations and for creating Incident Action Plans as needs arise. Additional municipalities are still being added to the system. Currently the plan is for DLAN to be used as the incident management system for Super Bowl 2022, which will be played at</p>

	SoFi Stadium in Inglewood, California. As other municipalities are onboarded the vision of real-time multi-jurisdictional situational awareness and collaboration will be fulfilled.
Project Start & Finish Dates	2021 - Ongoing 4 year contract

3.2 Vendor shall provide references for unique projects that started and/or were completed, and/or are in execution in the past Three (3) years.

Please see the answers provided in 3.1 above.

3.3 Vendor shall provide at least One (1) of the references above in 4.3.1.1 from United States public sector/government clients.

NYS Division of Military and Naval Affairs (NY DMNA)

NYS Division of Military and Naval Affairs			
Contact Person:	Staff Sergeant Robert Spohr		
Contact's Email:	robert.t.spohr.mil@mail.mil		
Address:	NYS Division of Military and Naval Affairs (DMNA) 330 Old Niskayuna Road Latham, NY 12110 United States		
Contact's Phone:	518-786-6104	Date of Service:	2009-Present
Modules:	DLAN Enterprise with: GIS Premium, Mobile Responder, Watch Command, Chat Client, Communication Center, Briefing Notes, ICS Forms, Incident Folders, Phone Book, Reference Library, Ticket Manager, Calendar		
Scope of Work:	<p>Summary: BCG installed a multi-functional DLAN system for this military operation to manage Army National/NY, State Naval Militia, Army Air Guard – Air Wing Military Operations, and Guard-Air Wing Military Operations. To address their numerous responsibilities and requirements they have many of DLAN’s optional Modules including: Watch Command, GIS, Reference Library, and Briefing Notes. The system was originally installed as customer hosted and in 2017, they opted to host it in the cloud. Recently the system has been utilized for the air operations activities for the Lake Ontario Flooding situation as well as recent COVID-19 responses.</p> <p>Details: Buffalo Computer Graphics, Inc. (BCG) was the prime contractor and managed the initial installation, training, and all enhancements and re-configurations since 2009. DLAN software is used in the Joint Forces Headquarters (JFHQ) for military and naval affairs in New York State. DLAN plays a critical role in the 24/7 Joint Operations Centre managing day-to-day requests and monitoring potential hazards for the New York State Army and Air Force National Guard as well as naval and maritime forces in New York. The system is utilized to manage numerous tasks and requests for assets. During COVID, DLAN’s work flow flexibility was utilized by also managing end-to-end requests coming from the Javits Center field hospital in New York City.</p> <p>The system was successfully utilized to manage assets and activities for air operations missions in the critical Hurricanes of Sandy, Irene, and Lee. The JFHQ is located in Colonie, New York a short drive from the capital of Albany where DMNA works very closely with the Department of Homeland Security and Emergency Services for the State of New York who also utilize DLAN for all incident management and preplanning activities in the State. The DLAN solution utilized by DMNA is a feature rich version of the software designed to provide comprehensive end to end Air operations management of inventory, equipment tracking functions. The Watch Command module</p>		

	functions as a 24/7 Joint Operation Centre watch point to log and manage potential or ongoing activities. It also serves as a dashboard to monitor a variety of incoming communications, which can be posted to actionable work order tickets. These singularly logged items in the Watch Command can be bundled together into a larger collective if the situation escalates. Alert information is also monitored from this module, including IPAWS messages.
--	--

3.4 Vendor shall provide a minimum of three (3) relevant references to demonstrate that it has proven experience in managing hosted/on-premises EMIS solutions at a statewide level. All referenced Solutions shall be currently operational in a production environment. This information shall be provided prior to contract award. The document provided as a reference shall include the state, organization name, point of contact, start and end date of implementation.

Please see the answers provided in 3.1 & 3.3 above.

Reference #1 Oregon Department of Human Services

Oregon Department of Human Services (ODHS) – Emergency Management	
State:	Oregon
Organization Name:	Oregon Department of Human Services (ODHS) –Emergency Management
Point of Contact:	Steve Pegram, Executive Director
Start and End Date of Implementation:	8/17/21-Present
EMIS Modules Implemented:	This is a DLAN Premium system with the following modules: Bed Tracking, Finance, GIS Premium, HICS Forms & Job Action Sheets, Special Needs Module, Chat, Communication Center, GIS, Incident Folders, Mobile Responder, Phonebook, Phonebook Premium, Reference Library, Resource Database, Social Media Basic, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Healthcare Industry Pack, ICS or IMS Forms Module, Incident Action Plan Module, Role Checklist Module, Situation Report Module, Damage Assessment Form, Report, & Board, Road Closure Form, Report, & Board, Role/Task Status Report & Board, Shelter Management Form, Report, & Board, and the Sheltering Module

Reference #2 NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)

New York State Department of Homeland Security and Emergency Services	
State:	New York
Organization Name:	NEW YORK STATE DEPARTMENT OF HOMELAND SECURITY & EMERGENCY SERVICES OFFICE OF EMERGENCY MANAGEMENT (DHSES-OEM)
Point of Contact:	David Smith, Operations Section Chief
Start and End Date of Implementation:	2004 - Present
EMIS Modules Implemented:	This is a DLAN Premium system. Modules include: Chat, Communication Center, GIS Basic, Incident Folders, Mobile Responder, Phone Book, Phonebook Premium,

	Reference Library, Resource Database, Social Media, Status Board, Status Board Builder, Ticket Manager, Ticket Manager Premium, User List, Emergency Management Industry Pack, ICS, IAP, Role Check list, Situation Reports, Damage Assessment, Weather, Separate Training Site, Watch Command
--	--

Reference #3 NYS Division of Military and Naval Affairs (NY DMNA)

NYS Division of Military and Naval Affairs	
State:	New York
Organization Name:	NYS Division of Military and Naval Affairs (DMNA)
Point of Contact:	Staff Sergeant Robert Spohr
Start and End Date of Implementation:	2009-Present
EMIS Modules Implemented:	DLAN Enterprise with: GIS Premium, Mobile Responder, Watch Command, Chat Client, Communication Center, Briefing Notes, ICS Forms, Incident Folders, Phone Book, Reference Library, Ticket Manager, Calendar

4. GENERAL REQUIREMENTS

4.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below. Contract Items must meet or exceed the mandatory requirements as shown below.

BCG asserts that it shall provide West Virginia Department of Emergency Management with a software solution and services that meet all mandatory requirements below.

4.2

4.2.1 Emergency Management Information System (EMIS)

BCG is the creator and sole provider of a commercially available Emergency Mangement Information System (EMIS) with the brand name of DisasterLAN™ or DLAN for short. The system is modern, effective, completely customer configurable, and has been in use by agencies, counties, and states across the USA and Canada since 2003. BCG provides regular updates to the software every ten weeks and provides all help desk, customer support, and services work in-house with our staff in the USA.

4.2.1.1 Vendor must provide an EMIS solution that features the following:

4.2.1.1.1 Incident Reports

- 1. The EMIS shall enable authorized users to create, update, and view incidents from browsers, and mobile applications.*

Incidents

DLAN can be used to track and manage incidents, trainings, exercises, events, and daily activities of any size or scope from browsers or mobile apps. Whether used to manage a pre-planned event, severe weather, a crisis

situation, routine incidents, or a disaster, DLAN provides tools for incident tracking on many levels. With task, mission, and resource management tools, emergency communication tools, and custom status boards, DLAN makes it easy to track, manage, and report on multiple incidents and events from one unified mobile ready solution. Incident security features allow administrators to easily lock down an event or incident to just the people that need access to it. When using DLAN to respond to multiple incidents at once, the confidentiality of data between incidents can be enforced using the incident locking system. This allows the user to be granted access to information within specific ongoing incidents in the system, while restricting access to others. Information can be shared between incidents, which allows selective sharing of information. Incident security features allow administrators to easily lock down an event or incident to just the people that need access to it. Filters within the system make it easy to look at data specific to the incident the user logged into, as well as giving them the ability to look at data across multiple incidents simultaneously. Filters within the system make it easy to look at data specific to the incident the user logged into, as well as giving them the ability to look at data across multiple incidents simultaneously. Individual events are logged in the system as tickets within a designated incident. These tickets contain a variety of information as the customer chooses and can also be color-coded for status and priority in the system so administrators and users can quickly see the status. Issues can be quickly logged in an incident as a ticket with simple guided entry data entry tools. Task for ticket completion can be automatically assigned and routed to a responsible individual or Role through automated custom work flows in DLAN. DLAN provides simple color-coded ticket statuses and priorities for tracking and rapid status overviews.

Incident Creation

Incident Configuration allows an administrator to easily create, set security settings, and archive emergency incidents and planned events from a desktop or mobile device. Incidents can be created using either a traditional form or wizard interface. Active incidents are available for designated users to log in to and all data entered is tagged with the incident for management during and after the incident. This helps with creating after action reporting (AAR). In DLAN an Incident is defined by following government standard ICS and NIMS guidelines.

DLAN can run multiple simultaneous incidents and supports all levels of incidents from local, county, regional, state/provincial, and federal levels. The Lock-Down Incident Security feature allows separate incidents to be created for different groups, agencies, or municipalities with access restricted to only their users. Administrators can also set the default incident for users to log in to and can view and access archived incidents and events.

Administrators can send out automated notification messages to selected distribution groups when a new incident is created or when an incident is edited. They can also set the default incident for users to log in to and can view and access archived incidents and events. Another major feature of DLAN's Incident Configuration function is the ability to run a spot report or create an after-action style hot-wash report. Incident reports are comprehensive chronological reports detailing all additions and modifications to records and data that occurred during an incident or event. Reports can be filtered down to a specific date range or type of records, including tickets, messages, broadcasts, Status Board items, uploaded Incident Folder Documents, Situation Reports, ICS Forms, Incident Action Plans, and GIS Map Snapshots. Like other DLAN reports, the Incident Report can be exported or printed as needed.

When an incident is over it can be Archived by the administrator. At that point when an incident closed it is considered complete and no more information can be logged for the event. The information can still be accessed by select individuals with the GO-TO function. The Archived incident can be utilized for a variety of after action reviews including: recovery activities, reporting, or financial reimbursements.

Task & Mission Management

Task Management is achieved in the DLAN system with the Ticket Manager module. Each task or mission in the system is represented by a ticket. Tickets can include other associated elements such as forms, maps, checklists/guides, attachments, and other data. The module also has a full suite of progress tracking capabilities

including the ability to select a ‘type’ and ‘kind’ to help categorize the ticket and the ability to set statuses and priorities. Tickets can be tasked to a role that is responsible for updating or contributing to the ticket. Tasking is achieved by routing the ticket to one or more roles – this will make the ticket appear on the dashboard homepage for users in that role.

Built in to DLAN is the ability to log issues as individual ‘tickets’ with guided data entry tools. Tickets can be assigned as tasks to roles manually or with automated custom workflows and their progress can be tracked with customizable color-coded statuses & priorities within the Ticket Manager module.

Mobile Application

The Emergency Management industry is rapidly shifting towards mobile centric operations; with support for almost all devices, DLAN ensures you won’t be left behind. With DLAN, mobility is not an afterthought. BCG engineers approach development with a “mobile first” perspective where modules and pages are built to operate on tablets and phones early on in the development process. From there, DLAN engineers build our modules so that they are responsive; automatically scaling their capabilities, views, and features based upon the screen size of the end user’s computer or mobile device.

These “mobile first” methodologies also follow through with our reporting and exportability of data, allowing users to make use of information in the field even when the user cannot be on DLAN. All DLAN data, including reports, maps, emails, and images, can be exported using common exporting formats such as PDF, Word, Excel, and CSV, which can be read by most wireless handheld devices and laptops. These reports can be instantly sent to mobile users via email, Twitter, or other multimedia pathway.

In general, DLAN is accessible on any mobile browser that fully supports JavaScript, session-based cookies, HTML 5 technologies, and other modern web browser features. Some mobile devices that support DLAN natively (i.e. no app required) include, Apple iOS devices, Windows Mobile devices, and Android devices.

All areas of DLAN work within a mobile environment when connected to a Wi-Fi or cellular network. DLAN also includes a specific Mobile Responder App that can be used when unable to connect to a network. The app is designed for iOS, Android, and Windows and is available from the Apple App store and Google Play store.

The app stores all report data locally on the device and automatically sends it to DLAN whenever a Wi-Fi or cellular internet connection becomes available. This "store and forward" capability ensures data integrity and usability under the most adverse conditions. The app includes the ability to use either standard or custom forms. Filling out a mobile form using the app is a quick process completed by filling out fields, attaching photos or videos, and clicking the Submit button.

2. The EMIS shall geolocate the incident based on the incident location data and update the Common Operating Picture (COP).

The DLAN EMIS automatically geolocates all addresses entered into the system for incidents and other records. Additionally, entering an incident, also allows users to draw a point, line, or polygon (shape) on the map if an address location is not available. Geolocation tools in the system support multiple geocoders from different sources such as ESRI or local geocoders created by WVDEM’s GIS department. Because incidents (as well as all other records such as contacts, facilities, assets, and more) are geocoded, they all appear on the GIS Common

Operational Picture Map automatically without any additional steps needed to make them available. Users can toggle incidents, tasks, resource locations, and other data on or off to customize the map as needed.

In addition to incident location data, the COP can also be incorporated into a DLAN EMIS Status Board (dashboard). Status Boards consist of configurable panels that display information from various sources. Panels can be made up of situational awareness information, including messages, PDFs, images, social media feeds, Mission reports, and task reports. Additionally, Status Boards can incorporate saved GIS maps with preset data layers, basemaps and extents, animated weather radar imagery, links, websites including other DLAN pages, and more. All content is live and continuously updates for real time on the COP for situational awareness.

3. *The EMIS shall receive, record, and log incident situation reports submitted by authorized users. These reports may contain but not limited to the following personal identifiable information (PII):*

- 4.2.1.1.1.3.1 *First Name*

- 4.2.1.1.1.3.2 *Last Name*

- 4.2.1.1.1.3.3 *Phone Number*

- 4.2.1.1.1.3.4 *Address*

The EMIS solution will not store medical records or other data related to a person's health conditions.

DLAN's Ticket Manager Module includes a unique ticket forms feature for logging incident situation information and is able to receive, record, and log incident situation reports submitted by authorized users. These reports may contain but not limited to the following personal identifiable information, including: first name, last name, phone number, and address.

Ticket Forms can be created, uploaded, and edited by system administrators and help to standardize user data entry. These fully customizable forms allow administrators to decide exactly what information they want collected for particular types of incidents, requests, offers, tasks, reports, etc. Ticket Forms can contain any combination of fields, labels, grids, drop-down lists, and check-boxes that are needed in order to create a working electronic form that fits the needs of the organization. Ticket Forms can be associated with different ticket types and kinds, allowing for forms to be automatically attached as part of a required workflow when needed. Additionally, forms created by the user can be used with the DLAN Mobile Responder App. Offsite users can fill out and submit forms from the app (e.g.: damage assessment form) and it will sync back to the DLAN system automatically and be converted into an actionable ticket with the filled-out form attached.

The system allows users to report incidents using an online form. System forms are all secure, and can be submitted through the website or can be submitted from the Mobile App. Customer administrators can create their own incident report forms or edit the default ones that come with the system.

In addition to reporting incidents using a secure online form, users (or non-user stakeholders) can report an incident by email. Email messages sent to the system are automatically received and converted into a report ticket for reply or follow-up action.

4. *The EMIS shall provide a component to create, collect, and notify data related to different type of incidents that are reported through the Watch Center. These are the reports include but not limited to: Arson Investigations, Tip Rewards, Mine Incidents, Workplace Safety Tips, Safe Schools, Industrial Incidents, State Interoperable Radio Network (SIRN) operators' reports, and Infrastructure Protection*

Incident Notification (IPIN). The system shall allow the user to attach videos, photos, documents, and call recordings.

DLAN's Watch Command module includes 24/7/365 monitoring and communication tools to support Duty Officers & steady state operations. It provides the ability to receive up-to-date news and incident reports from staff and agency representatives across the state. Information is also aggregated from several external sources including incident reports into one internal location to facilitate the review and processing of information.

Ticket Forms, used in the Watch Command module will allow WVDEM to create data collection fields for use with incident reports. This means that users can select the incident report kind from a drop-down list (arson, tips, etc.) and then have relevant fields appear to guide the collection of further information. The form can be filled out from either the website or from the mobile app. The mobile app supports offline use and both the website and the app allow the user to attach photos, videos, documents, recordings, and other files. Forms can be created and configured as needed by WVDEM administrators or BCG support staff.

5. The EMIS shall enable the system users to change the status report and the system sends the report automatically as an email notification.

The system tracks incident reports as well as other information reports, donations, and requests, in a Ticket. The ticket interface includes key fields for managing information such as a priority field, status field, routing (assignment) field, and more. A user with can adjust the status of a report ticket by simply editing the ticket and clicking on the Status Field. This will open a drop-down menu from which the user can adjust the status. As soon as the user saves her or his changes, the status of the report will update everywhere in the system. Changes to report tickets, including status updates will trigger both internal notification s to users logged into the system, as well as email and text message notifications to users who are not logged into the system.

WVDEM administrators can control the list of available statuses, which users can change report statuses, and the rules regarding how automatic email notifications work.

6. The EMIS shall select from a dataset the right contacts who receive the email notification.

DLAN supports user alerts via multiple methods including both in-app alerting, external email and SMS notifications. Alerts can be triggered manually, or automatically based on system configuration settings. Email notification settings can be configured by WVDEM administrators on a user account basis, on a role/position basis, or on a system-wide basis. This solution offers a effective combination of ease of use and granular flexibility as needed. Examples of email notification capabilities are listed below.

Note: For privacy law reasons, users can opt-out of automatically triggered alerts to their email or text message device. However, in-app alerting to users who are logged into the system will always notify users.

Incident Event Alerts:

When a new incident or event is created in the system, the initiator can choose to trigger a notification as part of the incident/event creation process. The notification can be sent to users within the DLAN app (in-app) via DisasterLAN Mail (DMail) message which will appear in the user's mailbox, or it can be sent out to external contacts using email, SMS via SMTP (text message), distribution group, scenario contacts list, system to system

integration, IPAWS, or other communication channel. Incident and Event Alerts can also be configured to trigger automatically to any of the methods listed above based on system settings/rules.

Resource Request Ticket Alerts:

Automated email and text message notifications can be sent to users when a Resource Request has been tasked to their role but there is nobody logged in to handle it. Users who have access to that role will receive an email or text message notification (according to their preference) alerting them to this and providing a URL link to login and view the information.

Mission / Task Ticket Alerts:

Automated email and text message notifications can be sent to users when a Task or Mission Ticket has been routed to their role but there is nobody logged in to handle it. Users who have access to that role will receive an email or text message notification (according to their preference) alerting them to this and providing a URL link to login and view the information.

Other Requests/Polling of Stakeholders:

Agency Report Notifications: Automated email and text message notifications are also available for situation reporting. If a role has been tasked to complete an agency report for their role or organization and they have not completed it by the time the end of the operational period approaches, then users in that role will receive an automated notification asking them to login and complete their agency report.

DLAN also provides a number of methods for both automated and manually triggered notifications.

Accept Remove System: When a manager or authorized user assigns a task ticket to one or more roles, the receiving roles can use the accept/remove feature to either accept responsibility for completing the task, or remove themselves from the routing list which will decline the task and remove it from their role-specific view. Of course, an administrator or authorized user can re-route the task to a role after they have removed themselves. This feature is often used to poll several roles or agencies to see who can supply a resource or has the current capacity to complete a task.

CC Alert Feature and Email Reply

Notification Profiles: Users or administrators can create contact records for people in the DLAN phonebook. Part of the contact record allows a user to choose notification methods such as cell phone, email, SMS (text message), pager, etc. These contact methods are used when sending a manually triggered notification message.

Notification Distribution Groups: DLAN allows an administrator to create distribution groups which can be used to send outgoing messages. These distribution groups can be used to send an email, ticket, incident action plan, or ICS form.

Notification Scenarios: Scenarios work similarly to notification distribution groups, however, they allow an administrator to tie a distribution group to an emergency scenario. The concept is to allow preplanning personnel to create a list of people to contact in case a specific emergency occurs. Then a message can be

blasted out to contact all the right people immediately. Common scenarios are Severe Weather, Hurricanes, Tornadoes, Hazmat, Flooding, Train Derailment, Mutual Aid, etc. As long as WVEMD knows who they need to contact in a specific scenario, they can create a notification contact list ahead of time and this will allow them to gear up the EOC with the right folks during an emergency without having to spend the time to organize a contact list of necessary participants and call everyone.

7. The EMIS shall offer a mobile application and system interface to update the contacts notification dataset.

The EMIS includes native mobile applications for Apple iOS devices (e.g. iPhone, iPad), Android devices, and Windows devices in addition to the mobile-friendly web-based user interface. Users can login to the system from a mobile device and update the contacts notification dataset as needed. These changes are reflected in real time in the system as well as for users who are logged in through the mobile app.

The system also automatically updates contact information in several cases. First, when a user logs into the system they are asked to confirm their contact information. Updates at the login screen are automatically propagated to the user account, user list, and other areas of the system. Second, changes to contact information in the system's Phonebook Module automatically propagate down to the mobile app's online/offline contact directory as well as to the system's address book which is available when selecting a contact for a message, email, or ticket/task assignment.

8. Depending on the type of incident, the EMIS shall pull data to auto-populate reports.

DLAN can pull data to auto-populate various reports. The reports are designed to support both emergency situations and day to day operations. Modules such as Ticket Manager can easily be structured to create detailed reports on tasks, requests, donations, reports of information, Action Plans, Situation Reports, and more. All reports reflect real-time updates. As soon as a user makes a change, all reports are updated automatically and relevant data is auto-populated. Additionally, all reports are searchable and sortable, and can be exported off the system using the export tool.

Many of the modules in DLAN allow users to create custom reports as well. BCG's easy to use tools allow administrators to lay out new documents, boards, forms, links, and other pages as needed, giving DLAN users a powerful way of managing the various reporting and input needs of each incident.

Landing pages or dashboards allow administrators to control what a user or role is directed to once logged into the system. Additionally, administrators and users can customize the content they see on these boards in an unlimited fashion. Boards can include additional custom reports that contain either standard or customized data. An example of this would be a map report on a board. Map reports can include auto-populated information, standard DLAN data (events, incidents, requests, reports, etc.), and can include agency, role or user specific data such as critical facilities, shelters, schools, etc.

9. The EMIS shall offer a mobile application and system interface to update those datasets required to auto-populate a report.

The DLAN Mobile Responder App provides a system interface for users to update datasets to auto-populate a report. The app allows users to fill out and submit forms from the mobile app that are then synced to the DLAN web application and are automatically turned into actionable tickets with all data from the report auto-

populated into the ticket report. This provides field staff with a way to submit resources requests, reports of information, damage assessments, and other types of data from the field using a native iOS, Android, or Windows app.

10. *The EMIS shall offer a system interface to update select lists, such as the agencies list and resources list. The system shall control names' duplication.*

The DLAN EMIS provides an administration interface to authorized users. The administration interface allows admins to update drop-downs, select lists, and other data fields and configuration settings as needed. All changes occur in real time and are available to users as soon as the administrator completes them. For example, a list of organizations, agencies, or roles on the system can be updated by an administrator and those changes will appear for users immediately. The administration interface typically checks for duplicate names or entries upon creation. Some modules, such as the Phonebook also have administrator reports that can be run to check for similar personnel or agency records using a fuzzy logic to provide a list of potential duplicate entries. The administrator can then choose which record to keep and which to remove.

11. *The EMIS shall offer the option to send those reports as part of an email's content (email body).*

The system provides the ability for users to send reports off the system as an email. Email reports can include the information as an attachment file, or as content within the body of the email, or both. Users simply click the checkbox next when sending a report to select which way it operates.

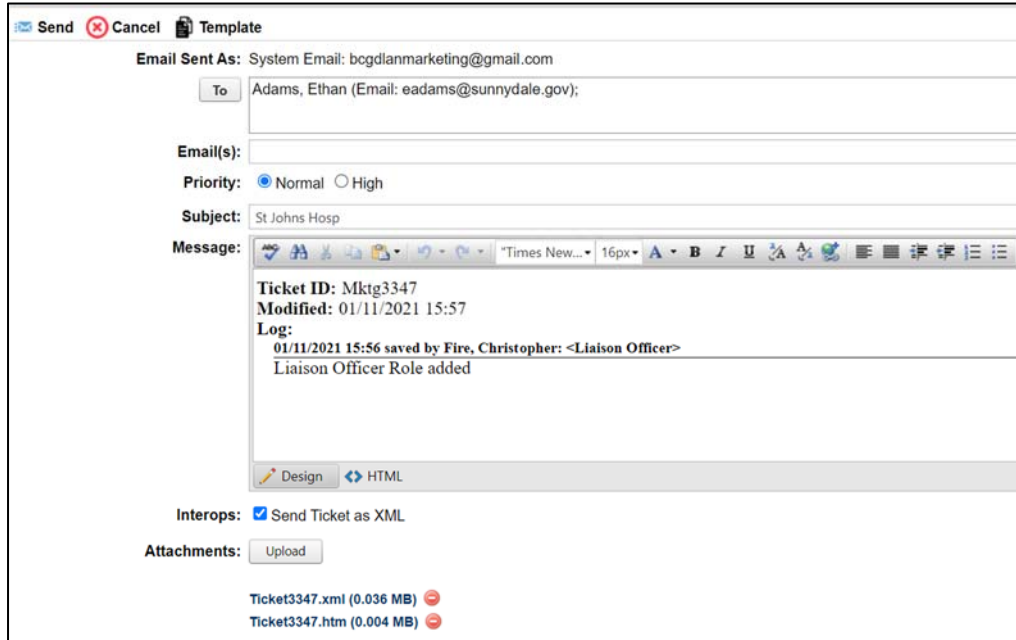


Figure 1: Email Reports

12. *The EMIS shall offer the option to call the phone numbers included in an incident report. It shall be possible from a mobile application and a system desktop/laptop/tablet interface. It is understood that the mobile device (phone or tablet) has a data plan.*

The DLAN system's mobile app allows users to call phone numbers that appear on the contacts tab of incident report tickets. For web-based users, if your device browser has the capability to detect phone numbers, you are able to call those numbers included on incident reports in DLAN.

13. The EMIS shall offer the option to print incident reports. The printed reports shall include images, and the attachments' list.

All incident report tickets can be printed along with images and attachments. Print options include the following:

- Print Table – this will print a tabular view of all incident tickets in the user's current report or view
- Print Ticket – this will print an individual incident report including any attachments such as images or associated files.
- Print Packet – this will print an individual incident report including all supporting evidence (images, files, forms, etc.) in a format that is suitable for use for reimbursement evidence.

Additionally, any incident report can be exported in PDF format and many can also be exported to Word, Excel, and CSV.

14. The EMIS shall geocode and present as a layer incidents per type of incident, and to include those layers in the COP. Those layers must be updated based on a data/time. It is understood the system is not replacing the whole dataset. It is updating based on new reports.

The DLAN system can geocode and present as a layer, incidents by incident type, and to include those layers in the COP viewer. The layers will be updated based on a data/time, and is understood the system is not replacing the whole dataset. DLAN updates based on new reports of information. DLAN's GIS module provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

DLAN's GIS functionality also allows you to fuse together geospatial information from virtually any external or internal source onto one common display. DLAN ensures that you are always viewing the latest information. User-friendly tools also allow users to interact with underlying data. For example, tools for identifying data and creating buffers based upon point features, polygons, or ALOHA plume models allow users to drill down and see information that is pertinent to the incident at hand. Data can then be used to make decisions, and if desired, exported for use in other applications.

From an administrator's standpoint, DLAN's configuration tools make managing and adding new data sources or basemaps quick and easy without needing any GIS expertise. Data can be organized into categories that appear on a touch screen friendly ribbon, making locating and toggling information on and off a snap, and data layers can be locked down to select users.



Figure 2: GIS Map Updates

Integrated Solution

In addition to incorporating key external data, DLAN GIS also displays data from other DLAN modules automatically. For example, incident report data entered in to a ticket appears on the map as a layer automatically. Incident report layers are created automatically based on Ticket Manager Module report criteria such as incident type, category, date/time, and other filterable criteria.

Additionally, users can add and edit incident report tickets directly from the map interface.

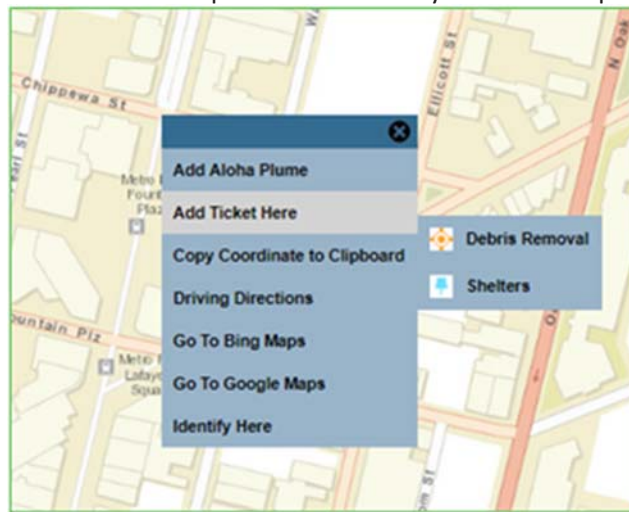


Figure 3: GIS Map Requests and Reports

15. The EMIS shall offer a dashboard per report type to monitor the notification status, access contact information per report type, and link to the datasets that are required to auto populate a specific type of report.

The DLAN EMIS Ticket Manager Module allows users and administrators to create custom reports of information based on filterable criteria including report type (incident report ticket kind). When the ticket manager report is created the user can select the columns of data that will be displayed in the report including notification status icons, contact information, links, form data, field data, dates/times, and other information. Once created, the

data returned by each of these reports populates automatically and is be viewable in a tabular format, or in a Status Board (dashboard) format.

See section 4.2.1.1.2 for more information regarding the Status Board Module dashboard capabilities.

16. The EMIS shall offer the option to export data as a .csv or .xls format.

DLAN includes an export feature that is available on all data tables, lists, and reports. With one click users can export data out of DLAN to MS Word, Excel (.xls), CSV, or PDF formats for further analysis. Data can also be emailed to outside stakeholders by clicking the Forward button. This attaches the document, file, or ticket to an email and sends it off the system to the selected or entered recipients.

4.2.1.1.2 Incident notification. The EMIS shall support automatic notification and support organizational as well as external email addresses.

DLAN supports automatic user alerts via multiple methods including both in-app alerting, external email and SMS (text message) notifications. Alerts can be triggered manually by a user sending a message or forwarding content to an email address. Additionally, notifications can be sent automatically based on system configuration settings. This includes the ability to automatically send out incident information to users who are offline, or based on business rules.

1. The EMIS must enable authorized users to assign or remove members of the contact lists to associated message groups to facilitate rapid dissemination of messages to specific sets of recipients.

DLAN allows authorized users to assign or remove members of contact lists to associated message groups facilitating rapid dissemination of messages to specific sets of recipients. Distribution Groups are an easy way to incorporate a set of contacts into one easy selection when sending out a message from the DLAN Communication Center. Distribution Groups can consist of DLAN Users, Phonebook Contacts, Custom Recipients, COG's (Collaborative Operating Group's), or any mix of them all. Distribution groups can be used to send an email, ticket, incident action plan, or ICS form.

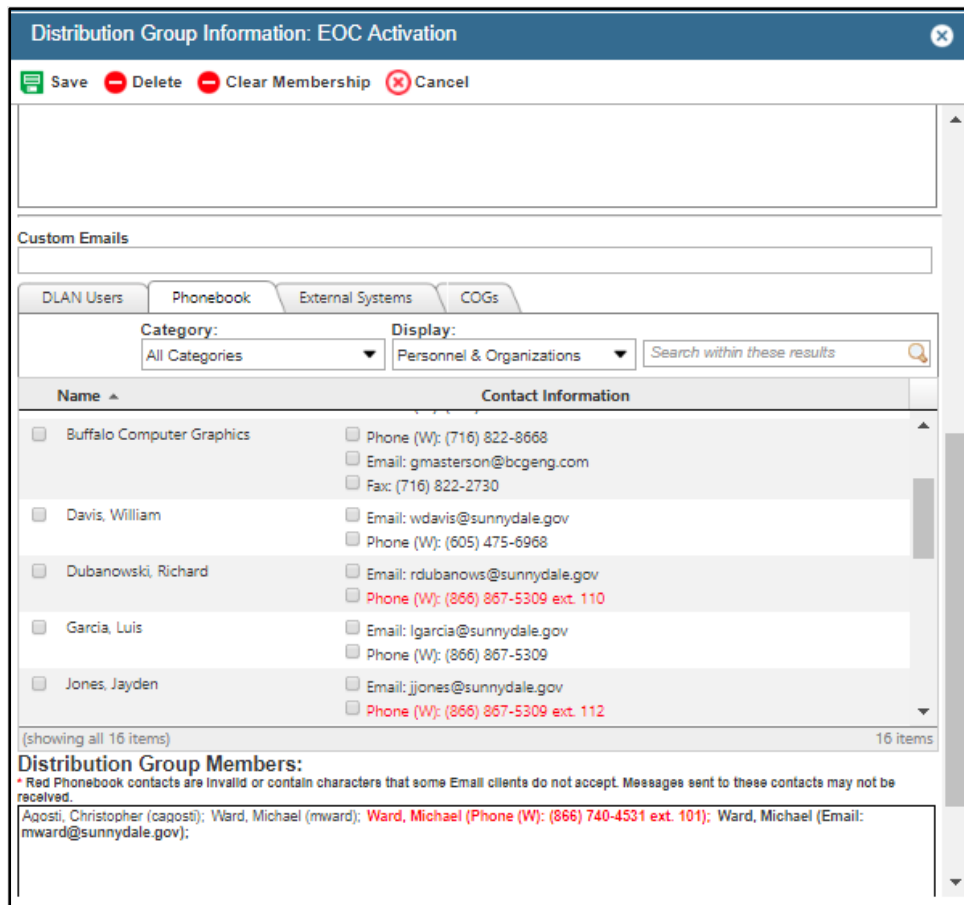


Figure 4: Distribution Group

4.2.1.1.3 *Contact lists and Directory. The EMIS shall enable users to create contact lists for emergency management staff and external contacts.*

DLAN’s Phonebook allows users to quickly create contact lists for emergency management staff and external contacts.

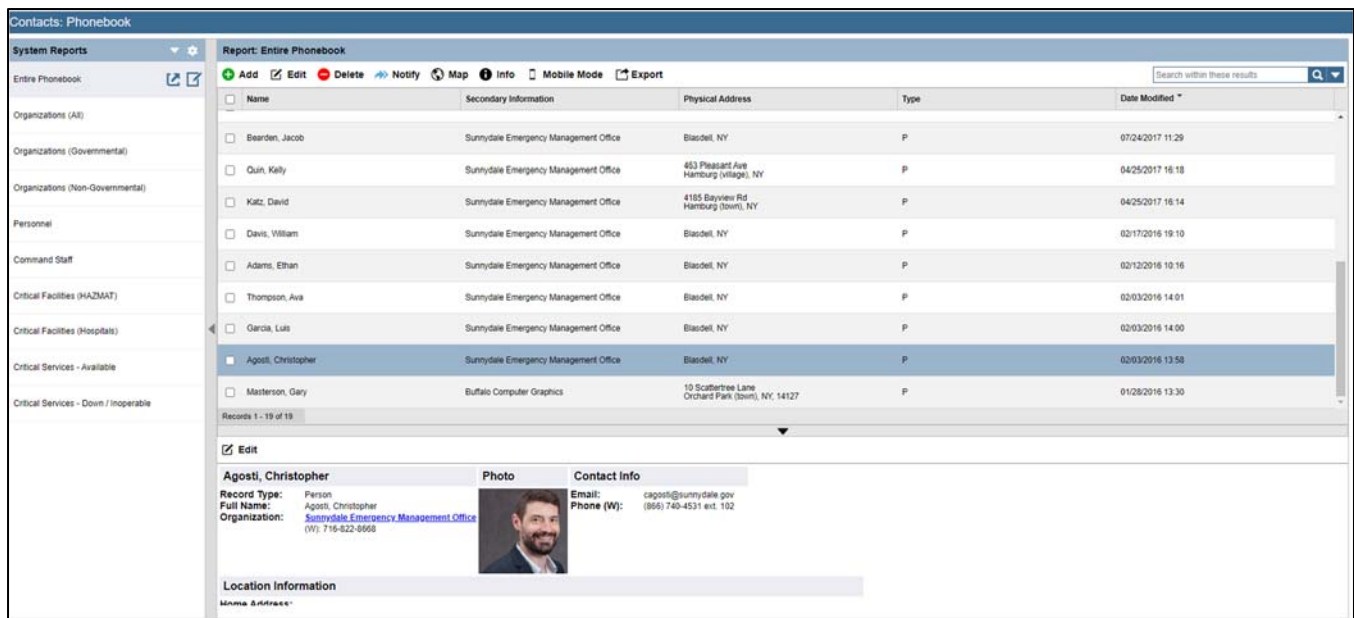


Figure 5: Phonebook Report

DLAN's Phonebook report engine allows users to easily create reports on personnel and critical facilities that are important to them. Tools allow reports to be created based on filters such as trainings, skill sets, categories of personnel, categories of facility, and locations. Once created, these reports immediately become available for use in other modules, such as GIS Premium or Status Board Builder. They can be used as layers on maps, bookmarked locations in map reports, and panels in status boards or landing pages. With this feature you can easily build real time views of staff that have specific qualifications, facilities that provide particular types of services, vendors that provide a required resource, and other types of critical facility reports that would be beneficial during an incident.

These lists can also be turned into distribution groups for easy messaging, see 4.2.1.11. for additional details.

1. *The EMIS shall use these contact lists to send reports, email, and notifications.*

The Notify button in the DLAN Phonebook allows users to notify some or all individuals listed in a Phonebook Report. For example, a phonebook report can be created to show all users on the system from a specific jurisdiction, or with a specific skill or training (e.g. firefighter, ops section chief, etc.). Then the user only must run the report to return the relevant records, click the checkbox to select them, and click Notify to send an email, report, text message, or notification to those individuals.

2. *The EMIS shall eliminate the duplication of effort by enabling users to update contact data one time and update the instances where that contact is used.*

Updating any contacts in DLAN's Phonebook automatically updates distribution groups and communication center recipients. This eliminates any duplicate of effort, and keeps contact data aligned and current for all users.

4.2.1.1.4 User-based permissions. This system shall be capable of assigning user-based permissions to data. These permissions will be based on security levels determined by system administrator(s). The system will be capable of determining access to data based on user permission level.

Security

DLAN includes a robust and flexible security utility that is part of the system administration module. It provides for multiple layers of security and access control throughout every level of the system. The permissions structure in DLAN is tiered and can be configured by the customer to have granular security permission, broad security permissions, or any range in between. DLAN accomplishes this flexible and intuitive security structure by implementing administrator defined security groups which are separate from user accounts and roles. These security groups are composed of several individual security permissions.

The principle of least privilege is the guiding methodology for security in DLAN. Users are only provided the minimum level of access necessary to perform their job functions in the areas of the system that they are required to use. Other areas of DLAN remain invisible or inaccessible. In addition to securing information, this also simplifies the number of options on the end-user's user interface, which makes just-in-time training quick and easy. It also encourages an ICS based workflow process for handling information flow in the EOC as each end-user has a clearly defined job duty and passes information along to the next person in the chain.

Administrators may configure an unlimited number of user accounts, groups, and roles. Groups and roles may be assigned to a user account through the use of a simple checkbox system. Users may have multiple groups and roles if they are trained for multiple positions, this allows them to retain one account and toggle between views as needed. DLAN comes with several default security groups already created, and during the configuration period BCG trainers will work with you to create other security groups and user accounts as needed. Administrators can change user's security permission on the fly and it will apply instantly without the need for the user to log out. This flexible and intuitive security system will cover all of your needs and allow system administrators to change or add privilege levels on the fly during an incident.

Export Button

DLAN includes an export feature that is available on all data tables, lists, and reports. With one click users can export data out of DLAN to MS Word, Excel, CSV, or PDF formats for further analysis. Data can also be emailed to outside stakeholders by clicking the Forward button. This attaches the document, file, or ticket to an email and sends it off the system to the selected or entered recipients.

1. Functional structure. The EMIS shall enable approved users to designate groups of users, by name or by functional position.

DLAN administrators can create groups within the system. Groups are flexible and can be used to define a selection of individuals, an organization, department, functional position, etc. Groups can be used to provide security permissions and access to features, or they can be used to identify which groups of users should be able to view an incident, status board, report, folder, file, or document.

2. Incident management. The EMIS shall enable users to manage daily activities and to monitor and track all aspects of an incident or event.

DLAN is specifically designed to support daily operations and emergency response. DLAN provides several tools that can be used daily for normal operations, including event logging, social media monitoring, email monitoring, webpage/RSS feed monitoring, documentation library folders, role based briefing notes, and several other tracking tools. DLAN's robust toolsets will allow users to monitor and track all aspects of an incident or event.

3. Duty and Call Logs. The EMIS shall enable users to access Duty Logs and Call logs.

Duty Logs and Call Logs can be accessed through Ticket Manager Reports. DLAN is often used by Duty Officers to monitor escalating events. It can also be used by call takers as a call center system to log phone calls and information requests. DLAN provides full tracking of logs that are kept by all user positions under specialized ticket reports such as "Tickets Added or Edited By My Role."

4. User management. The EMIS shall enable the system administrator(s) to define roles, assign privileges to users, create, maintain and/or delete users.

Administrators may configure an unlimited number of user accounts, groups, and roles. Groups and roles may be assigned to a user account with a simple checkbox system. Users may have multiple groups and roles if they are trained for multiple positions, this allows them to retain one account and toggle between views as needed. DLAN comes with several default security groups already created, and during the configuration period, BCG trainers will work to create other security groups and user accounts as needed. Administrators can change a user's security permission on the fly and it will apply instantly without the need for the user to log out. This flexible and intuitive security system will cover all your needs and allow system administrators to change or add privilege levels on the fly during an incident. Administrators can also add or delete users with similar convenience.

4.2.1.1.5 Interoperability. Vendor shall provide a solution that could interface with common EMIS web-based solutions.

DLAN is interoperable with EMIS solutions at FEMA Region III States and other Neighboring states out of the box using standard communication and messaging technologies. For additional technical information, please see the response to question 4.2.1.2 above.

1. The EMIS must be fully interoperable with Emergency Management Assistance Compact (EMAC) Operations System (EOS) for all functions.

The DLAN system is interoperable with the EMAC Operations System. Through the DLAN Ticket Manager Premium Module, specifically the preparedness toolkit feature, the system supports EMAC including the planning process, creation, and implementation of Mission Ready Packages using FEMA NIMS Typed Resources.

2. *The EMIS can be integrated and interoperable with the resources management software implemented at the local level, the WVEMD resources management, and EMAC platform, and the Geospatial platform implemented at WVEMD. Currently, the WVEMD uses AssetCloud for managing assets and Inventory Cloud for WVEMD's warehouse items. The Geospatial platform implemented at WVEMD is based on ArcGIS platform.*

Integration with Local Resource Management Software

The system can be integrated with Asset Cloud, Inventory Cloud, or with resource management software used at the local level by agencies, departments or municipalities provided that those systems support standard protocols for data exchange such as links, email, CSV, EDXL-RM, ArcGIS, RSS, CAP, or KML. The system also supports an advanced rules engine interface for integrations that allow WVDEM administrators to automate the evaluation, triage, and assignment of information that comes in from integrated email sources.

Additionally, the system supports integration with these platforms using DLAN system APIs which can be made available upon contract award.

Integration with EMAC EOS platform

The system can be interoperable with the EMAC EOS system, provided that West Virginia is willing to sponsor BCG for that integration project. EMAC requires sponsorship by a State level entity before they will make APIs available to a vendor for interoperability. BCG has not included specific costs for this integration in our price proposal Exhibit A – Pricing.

Integration with GIS

- **ESRI ArcGIS based-** BCG has been providing ESRI based GIS Platforms since 2004 in DLAN. Our proven solutions are fully integrated into our DLAN Incident Management System and allow users to view and work with essential incident information on a map. As GIS software continues to evolve, BCG will continue to set the standard for user friendly incident management tools and fully integrated and interoperable solutions. There are currently two GIS versions available: GIS Basic and GIS Premium.

Visualizing incident data is an essential part of situational awareness, that's why GIS Basic is included in all DLAN systems. GIS Basic provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

- **Ticket Report Sync with ArcGIS** - In addition to incorporating key external data, GIS Premium also displays data from other DLAN modules. For example, resource requests entered into the Ticket Manager appear on the map, as well as other reports and requests. Users can even add and edit tickets directly from the map. Users can also view video from traffic cameras entered into Streaming Video.
- **GIS Premium** -requires a connection to ESRI's ArcGIS Server or an ArcGIS Online account in order to serve up basemaps, provide geocoding & geoprocessing, view data overlay services (layers), use/embed ESRI's operational dashboards into Status Boards, and provide geometry

services. If your agency already has ArcGIS licensing, DLAN can consume and leverage your existing services at no additional cost. DLAN's GIS toolset is compatible with ESRI's ArcGIS Server or ArcGIS Online.

Alternatively, if your agency does not have access to an ArcGIS Server or ArcGIS online, BCG can provide you with access to ArcGIS services. Please talk to your BCG representative for details. Access to BCG's ArcGIS server services includes basic ArcGIS online map services (basemaps, map services, feature services, geocoding services, geometry services, and geoprocessing services). If your agency would like to manage your own custom GIS layers, you will need your own ArcGIS Server or ArcGIS Online account. Additional licensing for custom ArcGIS services is not provided by BCG and is the responsibility of the customer.

3. *The EMIS must have the capability to interoperate with the State's financial administration system to report material transactions including order and receipt of ordered material. Currently, the WVEMD uses OASIS.*

DLAN can export resource reports to common formats such as excel and CSV which can be uploaded into the State's financial administration system. If a more automated approach is desired, BCG could develop a custom integration with the State's financial administration system, however, scope, schedule, and cost, would need to be determined depending upon what software the finance system uses.

4.2.1.1.6 *Reports management. This system shall supply situational reports on the following factors of emergency management: event and incident reporting; resource requesting and management; response inventory management; infrastructure reporting, including road closures, hospitals, shelters, critical infrastructure; damage assessment; Community Lifelines; and a section for documents, images, user directory, organization charts, etc. the situational reports shall be saved as digital format, and printable from the EMIS interface.*

Event and Incident Reporting

The DLAN system provides reporting for individual tasks, missions, and after action reports for emergency events or entire incidents. Reporting on individual tasks or missions (groups of related tasks) is provided through a report generator tool that allows users or administrators to search, use filters, select columns and data, and produce a tabular reports of all important information. Tabular reports can then be visualized as graphs or charts or broken down into statistics using the Stats tool.



Figure 6: Status Board with Stats

For reporting on the whole incident, DLAN includes an after action report tool that provides customizable AARs that produce a chronological report of every action taken by users during the emergency, including: resource request tickets, situational information update tickets, messages, status board (dashboard) entries, broadcast messages, situation report documents, incident action plan documents, file uploads, reference folder creations, and recorded GIS map screenshots.

Resource Requesting & Management

DLAN Ticket Manager Module allows users to request resources using a simple ticketing system and then routes requests to other roles on the system for fulfillment. A Ticket Wizard option makes entering a request a simple step by step process. Resource requests routed to a user’s role will automatically appear on their status board (dashboard) or in their Ticket Manager report. Users can triage request tickets including adding statuses, priorities, attachments, locations, contact information, and other valuable information. As tickets are completed they will fall off of the users’ dashboards or ticket reports, keeping information to a focused and management level. Ticket Reports allow users to view completed tickets or information routed to other roles for situational awareness purposes.

Figure 7: Ticket Wizard - Resource Request

Response Inventory Management

The DLAN Resources Stockpile Module will allow WVDHSEM to pre-populate known resources and inventory equipment into the system and assign them to the agency or organization that owns them. This stockpile inventory can then be referenced or searched with the “Find Match” button when entering a resource request ticket. Users entering the request or a user in a logistics role can use find match to pull up the contact record for vendors, suppliers, departments, or agencies that own that type of resource. This makes sourcing equipment a quick and painless process. Stockpile inventory can also be viewed when looking at organization records in the DLAN Phonebook Module to see what resources that organization or agency owns.

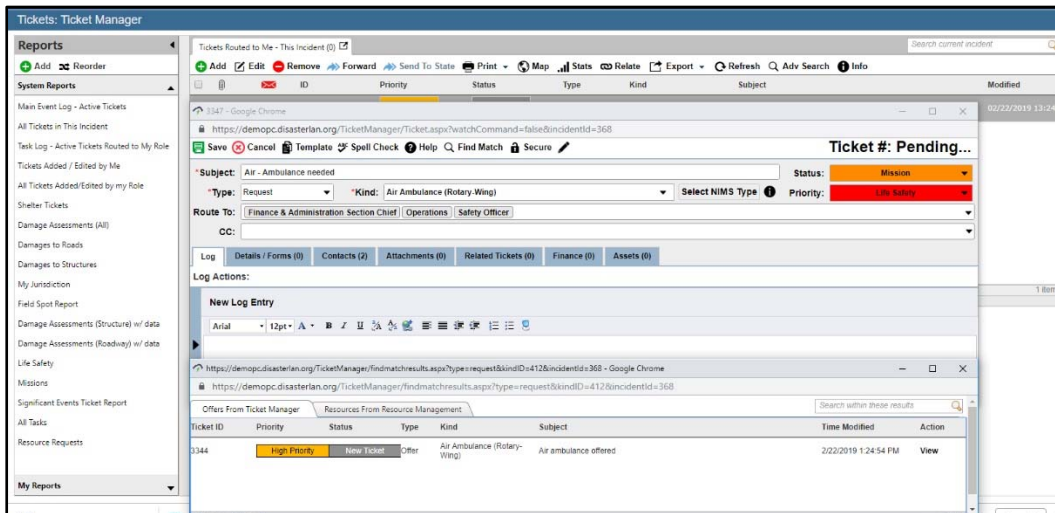


Figure 8: Ticket Manager - Resource Match

The DLAN Assets Module provides further tracking of inventory through the resource deployment, demobilization, and recovery phases of a resource request. Assets allows users to track the specific personnel or piece of equipment that was deployed to the field as part of a request, its current location, its status, images, and other key information on the GIS map. This asset tracking is also integrated right into the original resource request ticket, giving full visibility and accountability to the original requestor and managers that are coordinating resources. The Assets Module can also provide real-time AVL tracking for vehicles equipped with a tracking device or personnel using a GPS tracker. The DLAN Mobile app can also be used to track the location of personnel using the app, provided tracking is enabled on the device.

Infrastructure Reporting

- Road Closures

DLAN’s Status Board Module provides terrific visualization, coordination, and management of key information such as infrastructure reporting in a user focused dashboard. DLAN comes out-of-the-box with a Road Closure Status Board that is designed to populate information automatically from report of road closure tickets or road closure forms submitted from the mobile app. The board includes a tabular view of affected roads with columns for specific road closure data (nearest milepost, northbound/southbound, reason closed, etc.) color coded road status (open, closed, partial, etc.) and a map of the area displaying real-time traffic information from public sources such as ESRI and Google. This board is included with DLAN by default, but can be changed or edited by WVDHSEM as needed to display other real time road closure information.

- Hospitals

Hospitals can be tracked in DLAN Phonebook records which allow users to capture key facility information, resources, personnel, and other data. This can be viewed in the DLAN Phonebook, or in a Status Board (Dashboard) Panel. Additionally, DLAN offers a bed tracking module (not included in the direct cost of this proposal, but available as an option) which offers real time automated and/or manually updated bed status tracking

information, hospital facility capabilities, and bed occupancy information as well as ambulance transport tracking. Bed tracking is based on the Hospital Availability Exchange (HAVE) / HAVBED standard from OASIS.

In the recent past, DLAN has been used to integrate advanced syndromic surveillance report into the bed tracking and GIS map modules to show the top syndromes reported at area hospital ER departments, deviations, trends, ER capacity surges, and warnings related to public health. These integrations were implemented for the Ministry of Health in Ontario to track bed status and facilitate emergency communications between all 350 public hospitals in the Province.

- Shelters

Similar to BCG's Road Closures board, DLAN includes a Shelter board that is designed to pull in shelter information such as shelter name, location, capacity, etc. and display that data in a color coded tabular view in one visual dashboard. Users can edit and update shelter information from the board or submit entries through the Mobile App. As an example, staff on location working at a shelter can update their capacity details and have it sync that information in real-time back to the EOC where it will be displayed on the Shelter Board.

- Critical Infrastructure

The DLAN Phonebook Premium Module will allow WVDHSEM to track critical infrastructure and facilities in a record, capture point of contact information for a responsible person or agency, geolocate the facility to an address or point, and display it in both the Phonebook and on the GIS Map. Facility and infrastructure reports can be created dynamically as needed or pre-built. These reports can be used to color code facilities and infrastructure on the map based on their status (red, yellow, green, etc.). Finally, Assessments (damages, risk assessments, rapid assessments, spot reports, etc.) can be created for each facility and submitted through the Mobile App by field staff going out to do those assessments.

Damage Assessment

The DLAN Mobile Responder App is a flexible multi-purpose two-way communication and information reporting app that runs as a native app on iOS, Android, and Windows devices such as smartphones, tablets, and laptops. The App can be used for a variety of tasks including situation reporting from the field and task distribution, but its primary use case is for completing Damage Assessments and syncing that information back to the DLAN system. The Mobile App has a form based data entry solution, allowing WVDHSEM to design, build, and deploy any form that they wish to a user's mobile device. BCG provides a tried and tested Damage Assessment mobile form that is available out of the box. Users can open the app on their device and fill out a damage assessment on this standardized form. The app will automatically capture the user's location and provides the ability to use the map or an address to adjust it if needed. The app also allows users to take pictures and video and attach them to the Damage Assessment form. When complete, the damage assessment is synchronized back to the DLAN system. If the user does not have cellular or wireless internet connectivity the app will function offline and automatically syncs completed assessments once connectivity is resumed.

On the receiving end, DLAN comes with an out-of-the box Damage Assessment Status Board (dashboard) that populates a report and a map automatically as assessments come in from the field. Incoming damage assessments are automatically converted into actionable damage assessment report tickets and users can manage and update them through the Damage Assessment Status Board or their Ticket Manager page as needed.

Reference Documents

The Reference Library is DLAN's main file storage area and is designed to make files and documents available to staff anytime, anywhere. The Reference Library is not incident specific and designed to store persistent data that needs to be accessible for all incidents, such as policies, procedures, chemical and radiological reference information, emergency evacuation plans, or any other reference document. Three features that differentiate

DLAN's Reference Library from other file storage applications are that it is fully accessible from mobile devices; its intuitive security settings which allow folders to be locked down by the security group to protect sensitive information; and that it can be used to upload any type of file (unless specifically prohibited by an administrator).

The Incident Folders Module is a secondary file storage feature that works similarly to the Reference Library but is designed to save incident specific documentation, such as disaster scene photos, press releases, news articles, static GIS Maps, and agency generated documents. Documents uploaded to the incident folders during an emergency become part of the incident record and after action report. Incident Folders are archived when the incident is archived in DLAN. A pre-set folder structure can be defined and is auto-created for each new incident to create a consistent organizational structure for saving incident specific files. Other DLAN modules have quick-links to store items in Incident Folders or to post documents from Incident Folders to other modules, such as the Status Board. At the end of the Incident, all materials stored in Incident Folders can be downloaded, rolled into a report, or Emailed out.

User Directory

The DLAN User List Module shows which users are currently online/offline and provides a link to message them via DLAN Mail Message (DMail) or Chat message. The User List displays the offline or online status, proper name, username, current role (EOC manager, logistics chief, Red Cross liaison, etc.), Email, and phone number of each user. Users can filter the user list by showing either online or offline users for easier viewing.

Organization Charts

The DLAN Incident Action Plan (IAP) Module enhances the functionality of ICS forms by allowing users to compile them into IAPs following FEMA's guidelines. This includes the ICS 203 and 207 forms for organization charts. An IAP can be published with just the org chart form or as a compilation of any ICS forms that are useful for the current incident. IAP Templates allow users to select a pre-filled IAP org chart that already has key information entered. Or, the user can copy/clone a previous org chart and use it as a starting point for a new one.

1. The EMIS shall enable users to access situation reports and visual situation displays, and provide the means for visually presenting situational information in a dashboard and COP.

The Status Board is designed to display multiple types of situational awareness information in a dashboard format. It leverages both user updated content (e.g. incident messages) and automated external data sources (e.g. Twitter). All content is live and updates continuously for real time situational awareness. All board elements are interactive and the content view can be customized by the user for his or her current session without affecting other users.

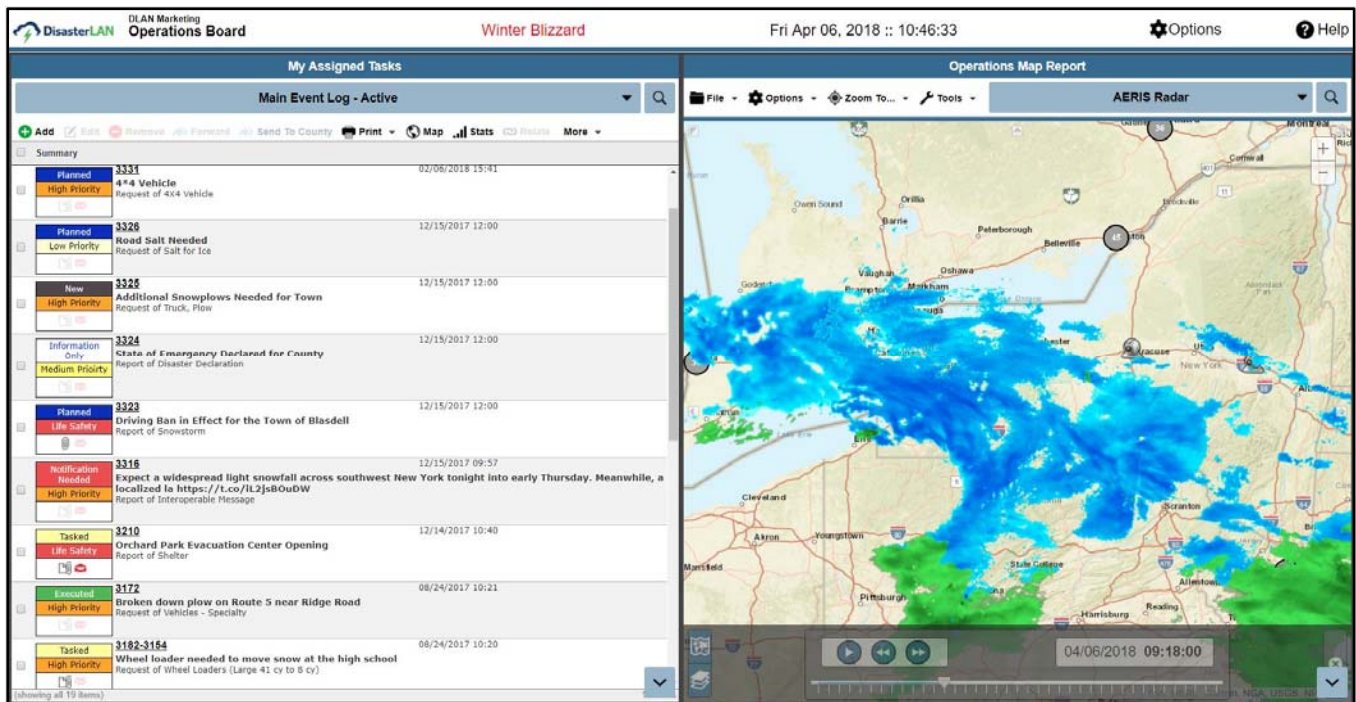


Figure 9: Status Board - Operations

Many subscription (data) types are available to populate each panel. Boards can also display user curated content such as critical decision messages. Boards can be created to display summary or detailed information from multiple incidents in one display. This mixture of different data sources and display types means the number of status boards an organization can make is practically endless, creating a truly customized experience.

The Status Board is specifically designed to be easily viewed on mobile devices, desktops, and projector/television displays. Each individual board panel can be popped out into its own window for full screen viewing.

2. *The EMIS must enable users to access Road Closure Notifications and reports from the West Virginia Division of Highways and display the information in the EMIS solution and the COP.*

DLAN is designed to be interoperable with many common information sharing technologies and can enable users to access Road Closure Notifications and reports from WV Division of Highways and other agencies from within DLAN. Data from 511, National Weather Service, and Twitter can be displayed on DLAN Status Boards. For example, the 511 and WV interstate feeds can easily be displayed. DLAN also supports the display of CAP messages, Atom feeds, GeoRSS, GeoJSON, KML and other sources that can be visualized on the DLAN GIS Premium Map. If none of these existing technologies meets the state's needs, then BCG can provide a customized integration point using our API.

3. *The EMIS must provide ad hoc user-defined reporting in which dynamic, real-time data reports are created by the user on an as-needed basis.*

Many of the modules in DLAN allow users to create custom reports. BCG's easy-to-use tools allow administrators to lay out new documents, boards, forms, links, and other pages as needed, giving DLAN users a powerful way of managing the various reporting and input needs of each incident.

System reports allow administrators to save reports that are accessible to all users, such as a "completed tickets" report showing only tickets in the incident that have been completed. Users can also create custom reports to show whatever information is of interest to them.

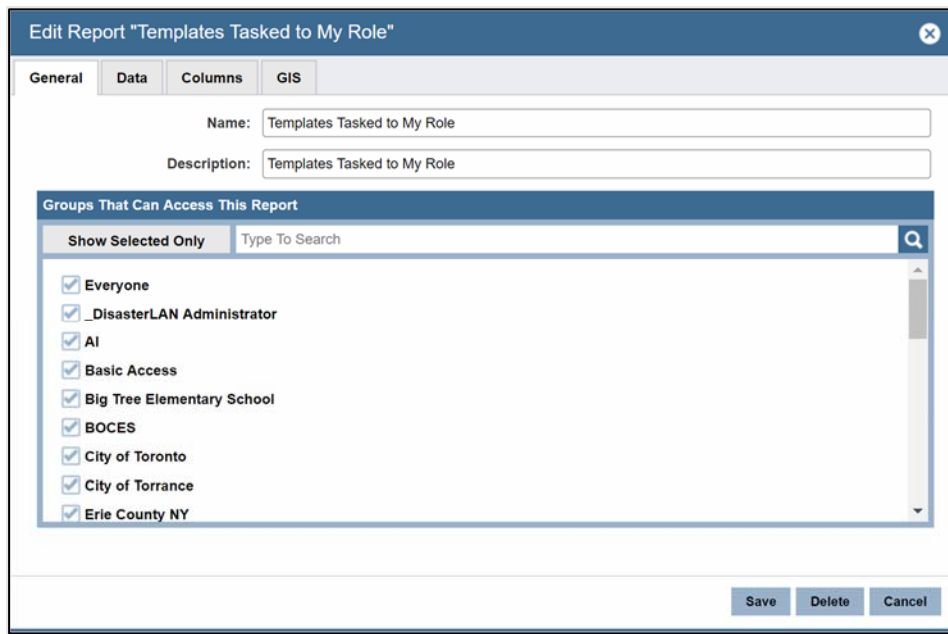


Figure 10: User Defined Reporting

In the Ticket Manager, ticket reports are used to filter the list of available tickets down into meaningful sets of similar tickets so that they can be more easily tracked, worked upon, and completed. Customized views of ticket data (reports, requests, donations, etc.) can easily be queried based on date, time range, incidents, priority settings, status settings, jurisdiction data, user submission data, location data, routing information, keywords, attachment data, and other information. Users can select the columns they wish to see in the report, using any data within the ticket or any dynamic forms created by WV staff. These queries can easily be saved for use by other groups of users in map reports, in ticket manager grids, status boards, or as personal reports. This ability to quickly filter and present data for temporary or permanent use allows the Ticket Manager to be a core data management system for customer displays and views on the system.

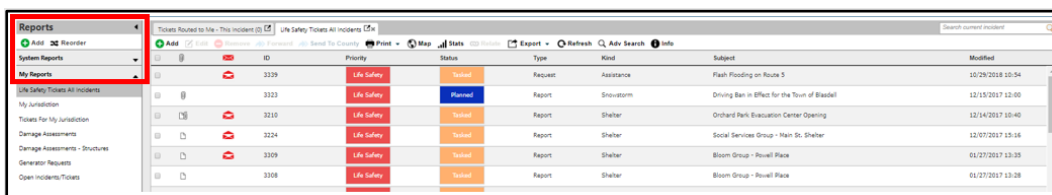


Figure 11: Ticket Manager Report

Like the ticket reporting tools, phone book data can easily be filtered by users to display organizations and people based on filterable criteria such as location, trainings completed, skills possessed, categories, text, and other filters. These reports can then be saved for use by other users on the system in order to easily find contact information on vendors and staff that is specific to their emergency management needs.

Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users.

4. The EMIS must provide data views that users can select based on parameter such as date, event type, counties. The data views should sort those views and enable the user to sort by parameter too.

Customizable views in DLAN allow all users to drill down to whatever data is most relevant to them, including the ability to search sort, sort, filter, and report on all data views.

Grid Views – DLAN ticket information can be easily viewed by selecting parameters the user is interested in. Information can be sorted, searched, and filtered on every data column or entry: such as date, time created, time modified, due date, event type and kind, location, tasking, etc. A simple click on a field or column provides the ability to easily sort and view information in the system. Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users

- Dates – Ticket Information can be sorted and viewed by Last Modified and other date information available on every record.
- Event Type – The event type is captured in the ticket’s Type and Kind fields. The lists are based on NIMS/FEMA types and kinds, but are customizable by West Virginia’s administrators. All this information can be selected and sorted for viewing.
- Ticket Reports – These reports allow custom views of data by user definable parameters such as kind, status, priority, contact information, location, dates, and other information displayed in the ticket.
- The Ticket Manager includes preconfigured forms for capturing additional resource request information and capturing information from off-site staff. It also includes preconfigured reports for easy access to essential information. Additional forms and reports can be purchased individually, or with Ticket Manager Premium you can build your own custom reports and forms.

5. The EMIS must provide detailed user access and activity reports.

DLAN provides detailed user access and activity reports as part of its standard System Administration Site Security reports set - as shown in the illustration below. The User List function will enable Administrators to view and report on all users currently logged into the system. Site Security Reports are also available to provide the following information:

- Currently Locked Out Users
- Currently Logged In Users
- Group Modules
- Module Users
- Portal Users

- Role Association
- Watch Command Activity
- Security Violations
- User Activity
- User Groups/Modules
- User Login History
- User Login Timeline
- User Last Changed Password

The screenshot shows a web-based report interface. At the top, there are input fields for 'Start Date: 3/19/2019' and 'End Date: 3/26/2019', along with a 'Run Report' button. Below this is a navigation bar with '1 of 1' and 'Export' options. The main title is 'User Activity Report From: 3/19/2019 11:26:59 AM To: 3/26/2019 11:27:01 AM'. The primary data is presented in a table with columns for Username, Phonebook Entries Added, New Calls Entered (Regular, Watch Cmd), Calls Modified (Add+Edit) (Regular, Watch Cmd), and Total Calls Modified (Add+Edit). Below this is a 'User Activity Summary' section with a smaller table summarizing totals for Phonebook Entries Added, New Users Added, New Calls (Regular, Watch Cmd), Calls Modified (Regular, Watch Cmd), Total New Calls, and Total Calls Modified (Adds + Edits). The footer indicates 'Printed on: 3/28/2019 11:27:01 AM' and '1 of 1'.

Username	Phonebook Entries Added	New Calls Entered		Calls Modified (Add+Edit)		Total Calls Modified (Add+Edit)
		Regular	Watch Cmd	Regular	Watch Cmd	
mward	0	2	1	2	4	6
bcg_cfire	0	0	1	1	1	2
All Users	0	2	2	3	5	8

User Activity Summary From: 3/19/2019 11:26:59 AM To: 3/26/2019 11:27:01 AM		
Total Phonebook Entries Added	0	
New Users Added	0	
New Calls	Regular	2
	Watch Cmd	2
Calls Modified	Regular	3
	Watch Cmd	5
Total New Calls	4	
Total Calls Modified (Adds + Edits)	8	

Figure 12: Sample Security Report - User Activity

4.2.1.1.7 *Geospatial component. The EMIS shall be capable of generating dynamic maps and reports that represent a COP. The system shall be designed and equipped to upload of the GIS information for spatial display in the form of shapefiles, layer files, web map services (WMS), and .kml or .kmz formats.*

BCG has been providing ESRI based GIS Platforms since 2004 in DLAN and in other products. Our proven solutions are fully integrated into our DLAN Incident Management System and allow users to view and work with essential incident information on a map. There is even a mini-map function built into the ticket/task entry screen and preview screens are available if you need to view tasks on a map. Map reports can be created and displayed on a dashboard/status board for easy viewing. Mark up drawing tools and the ability to save or share layers and mark ups is built into DLAN. Users with the appropriate permissions can create maps and reports from the GIS data in the system. As GIS software continues to evolve, BCG will continue to set the standard for user friendly incident management tools and fully integrated and interoperable solutions.

Visualizing incident data is an essential part of situational awareness, that's why GIS Basic is included in all DLAN systems. GIS Basic provides mapping functionality across the DLAN system, allowing users to view mini-maps in Ticket Manager, Communication Center, and in IPAWS messages. It also includes basic geocoding; reverse geocoding of points and polygons; location selection by point, polygon, line, or coordinate; and the ability to convert coordinates from one system to another (e.g. latitude/longitude to decimal).

External data sources for mapping include: Aeris Weather, Aloha Plume, AVL Trackers, CAD data via Email or custom API, CSV, Drone Imagery, ESRI ArcGIS services, ESRI Online services, Excel, GeoJSON, KML, WebServices and Shapefiles.

DLAN Module mapping data sources include: Asset Tracking Reports, Incidents & Events, Mobile Responder Phonebook Premium Reports, Phonebook Reports, Risk & Resiliency, Route Analysis, Streaming Video, Ticket Manager Premium Reports, Ticket Template Layers.

DLAN GIS works with ESRI's ArcGIS Server or an ArcGIS Online to serve up basemaps, provide geocoding & geoprocessing, view data overlay services (layers), use/embed ESRI's operational dashboards into Status Boards, and provide geometry services. If your agency already has ArcGIS licensing, DLAN can consume and leverage your existing services at no additional cost. DLAN's GIS toolset is compatible with ESRI's ArcGIS Portal/Enterprise or ArcGIS Online.

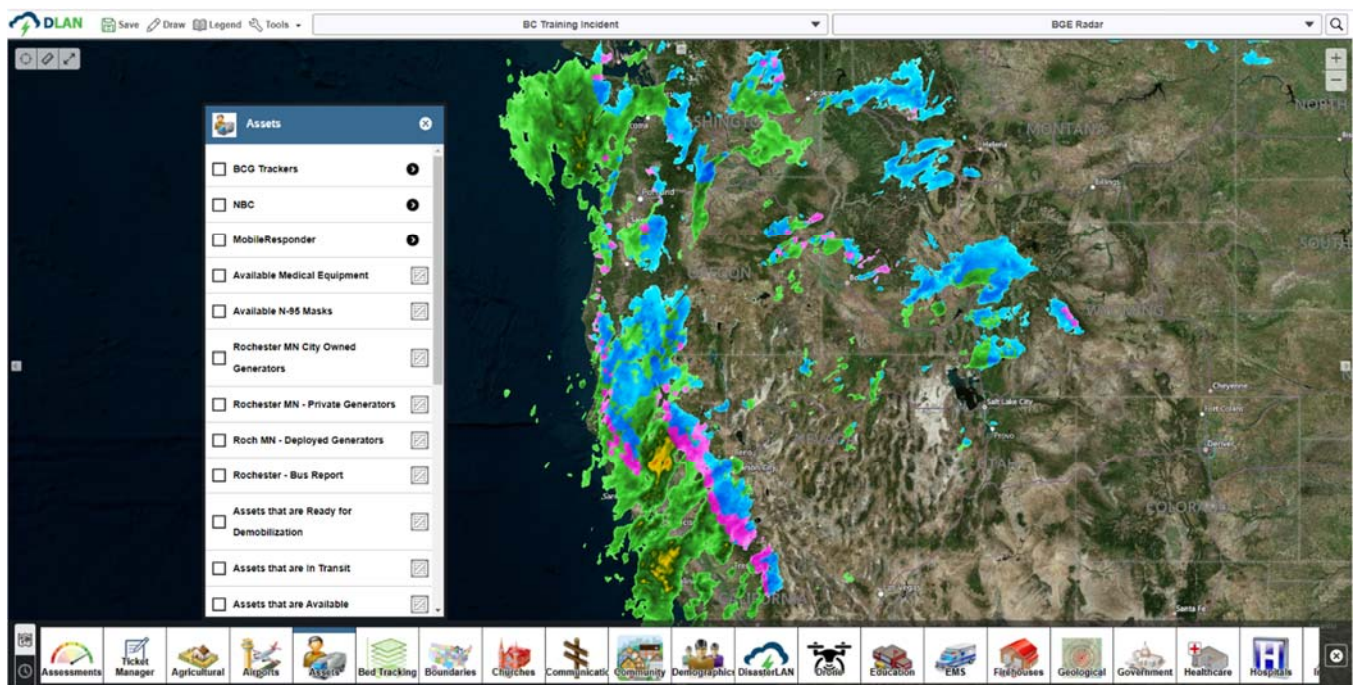


Figure 13: GIS Map Spatial Displays

1. *The EMIS's geographic component shall be capable of displaying a dynamic map identifying incidents, events, effects related to those events: and, the responding agencies involved, including agency contact information.*

All Incident and event can be illustrated on a GIS map in the system. The data that includes GIS information can be displayed and edited on a dynamic map. Additionally, as users interact with the system and add content such as incidents, events, effects, and responses/comments, the system automatically builds GIS layers out of that content which are visible on the GIS map and update in real time as users update the content. Examples include: incidents, events, tickets, facilities/organizations, personnel, assets and resource locations, assessments, weather data, streaming video, templates/mission packages,

2. *The EMIS's geographic applications shall allow users to add new layers to the dynamic map.*

GIS Administrators will have full access to the admin menu, which will allow them to customize features such as basemaps, overlays, layers, and categories.

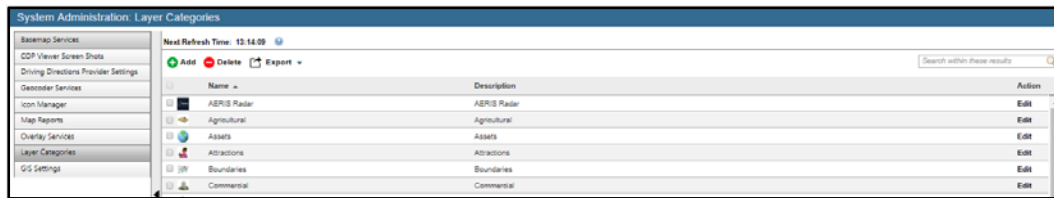


Figure 14: GIS Admin

3. *The EMIS's geographic application shall permit users to use the geographic analysis functions.*

DLAN's GIS module allows users to use a variety of geographic analysis tools and reports such as proximity indicators, finding the nearest point, and creating buffers to estimate possible human, property, and infrastructure effects. Additionally, the EMIS is integrated with ArcGIS products and can leverage the numerous powerful geographic analysis functions available through the ArcGIS platform. Any analyzed data can then be synced back into the DLAN EMIS system.

4. *The EMIS shall enable the user to edit and update layers, query multiple datasets, and export the query in GIS formats, tabular or delimited formats.*

GIS data can be organized into categories that appear on a touch-screen friendly ribbon, making location and toggling layer information on and off a snap. Additionally, data layers can be locked down to select users based on administrator configuration. The system supports the sharing and export of GIS layers and data to external recipients (outside of the EMIS) as CSV exports or KML.

5. *The EMIS's geographic component must have a geographic application capable of supporting the resource request management.*

DLAN provides all the tools necessary for the display and visualization of resource requests and supplies within the GIS Module. Maps can be used to display resource request locations. The mapping tools also allow the ability to view the status of resource requests and delivery locations of resources on either a map or table. Figure 3: GIS Map Requests and Reports displays a snapshot of a resource deployment ticket being updated directly from a Resource Location map. This solution also supports tracking of personnel resources through the mobile app with real time GPS tracking available on the GIS map for safety, tracking, and search operations.

6. *This geographic application shall contain dynamic maps for displaying information such as the status of resource request and delivery location. The dynamic maps must deploy in real time the resource request status on a map and in a table view. The application shall permit add, remove, and edit layers.*

DLAN's GIS dynamic maps and mapping tools allow the user to view the status of the resource requests and delivery location on either a map or table. GIS information is displayed in real time and includes the ability to automatically record changes in the GIS map from both user input data and automated data feeds. Data can be organized into categories that appear on a touch screen friendly ribbon, making location and toggling layer

information on and off a snap. Additionally, data layers can be locked down to select users based on administrator configuration.

Data for Resource Requests including status are visible in a table view in the Ticket Manger module and in a GIS map view as a layer in the GIS Map module. A WVEMD administrator can add, remove, and edit layers as needed through the system administration pages. All changes are reflected in real time.

7. The EMIS shall permit dynamic search by address, toponyms, coordinates, and resource type. The application shall work on computer, tablet, and mobile devices.

DLAN's GIS Mapping tools and search dynamics allows users to search by address, toponyms, coordinates, and resource type. All table views / data grids in the system can be searched and sorted and will return any data that appears in the table. Additionally, all areas of DLAN, including the Map and dashboards scale to work on desktop computers, laptops, tablets, and mobile devices.

8. The EMIS's geographic component must include and integrate mobile applications to collect, present and disseminate data and information.

With DLAN's Mobile Responder App, emergency managers in the field can easily communicate essential information with each other and back to the EOC using their mobile devices. The App is designed for disaster area use and can function regardless of connectivity. The simple form interface makes the app ideal for data collection- including damage assessment, debris management, and spot reports from field staff. Using the Mobile Responder, users can send data, images, and videos from their mobile devices into DLAN.

Once a form is received by DLAN, it can be reviewed and posted to a ticket or submitted to the Risk & Resiliency Module. Alternatively, mobile forms received by DLAN can be posted to a ticket automatically based on business rules. This gives users the power to then run reports on damages, map locations, and assessment information and share it with interested parties within or outside of the EOC with no need for double data entry or phone calls.

Offline Functionality

The Mobile Responder App allows field staff to work offline with any mobile form on their system. The App stores all report data locally on the device and automatically sends it to DLAN whenever connectivity is reestablished. This "store and forward" capability ensures data integrity and usability under the most adverse conditions.

Assigned Task Mode

DLAN simplifies the user experience by focusing their attention on only the tools they need to do their job. The Assigned Task Mode in the Mobile App helps get field workers started on their daily duties quickly. The App can now automatically sync and download all the tickets assigned to a field worker (routed their role) when they first log into the app. This includes all information the field worker needs to do his or her job, including forms, basic ticket data, and contact information for the person who assigned them the task as well as contacts for the job

location and anyone else assigned to assist on the task. Additional tasks can be pushed to a field worker in real time and completed ones will synchronize to DLAN when published. If the field worker enters an area with no cellular or wireless connectivity they will still have all their assigned task data to work with offline. When the worker returns to an area with connectivity, the App automatically publishes their completed assignments to DLAN.

The Mobile Responder App is included in our DLAN Advanced and Premium editions, as well as in all of our industry packs; it can also be added to any DLAN System as an option. The App can be downloaded for free from the Apple App store and Google Play store; authorized DLAN credentials are necessary to use the App.

9. The EMIS must enable users to track incident locations and information and develop trend data over time during and incident.

As the record changes in the GIS map from both user input data and automated data feeds; it also snapshots an image of the map change, and saves it to the incident record. This allows WVEMD to review what the historical map looked like at point throughout the incident, and justify or reconfirm any decisions made based on geospatial situational awareness. Authorized users can view a chronological record of geospatial changes throughout the incident to help identify trends.

4.2.1.1.8 Training. The vendor shall provide all training opportunities leverage against the State's development and training platform of the EMIS solution. The vendor shall provide training for:

BCG can perform all training and exercises using the State's DLAN Development or Test Site. The Development Site can also serve as a test bed for new releases and updates so that the State can test them in a controlled environment before applying the update to the production EMIS site.

1. Users.

BCG will provide onsite instructor-led basic user course training for these users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

2. Trainers.

BCG will provide basic, advanced, and administrator course training for these users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

3. System Administrators.

BCG will provide administrator course training for these individuals. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

4. Technical Staff, to include Information Technology, Programming, and GIS staff.

BCG will provide a technical training for these users. BCG will also provide necessary knowledge transfer during project implementation to assist these technical users. Training includes a course agenda, quick reference guide materials, and a recording of the training provided afterwards.

4.2.1.1.9 The Vendor shall make training available on-site for all user levels. The vendor shall identify the following:

BCG will make training available at the State for all levels of users of the DLAN EMIS as part of the EMIS project implementation. BCG trainers are not just experts in the technical aspects of the system, but also in its applications in emergency management. All our trainings will be tailored to WV's specific organizational workflows and DLAN site configuration

1. Course names (Serialized and in Sequential organization order)

Onsite, instructor led training broken down into:

Administrator Training

- General DLAN Functionality overview
- New Incident Creation
- User & Role Management
- Security Groups and Record Security
- System Setup and Configuration
- Module Administration
- Status Board Building
- Form Building
- System Reports Creation
- Workflow Creation

Basic User Training

- Introduction to DLAN
- Login & Navigation
- Landing Pages and Status Boards
- Ticket Wizard
- Ticket Manager
- Mobile App
- Communication Center
- GIS Mini-map
- Calendar & User List
- IAPs, Phonebook, Resources, & Assets
- Ticket Manager Premium, Templates
- Resources & Assets
- Communication Center External Messages
- Status Board Content Curation
- IAP Creation
- Situation Report Creation
- GIS Premium Map Viewer
- User Reports Creation

Training Materials Provided:

- Training Agenda for basic, advanced, and administrator training courses
- Training Quick Reference Guides for all DLAN Modules owned by West Virginia
- PowerPoint or Video Recording of training courses

Additional training resources included:

- DLAN Online Help Articles
- DLAN Reference Library Materials (storage for all current quick reference guides and training materials)
- DLAN In-Board Help (Situation Report Builder Board & IAP Builder Board)

2. *Delivery Methods*

Training delivery methods typically include onsite instructor led training using a mixture of lecture and hands-on activities where students perform operations and exchange data with others using the DLAN software. Training can be delivered either virtually or at WV's facility of choice.

Alternative services: BCG can provide virtual trainings, webinars, one-on-one coaching, train the trainer sessions, custom training videos, and custom training documents to meet West Virginia's specific needs.

3. *Length of each course*

The DLAN Administrator Training Course is designed to run two full days for a state level system. Time may vary slightly depending upon the number of modules and features included in the State's DLAN system.

The DLAN Advanced User Course typically runs one day.

The DLAN Basic User Course is designed to run one full day session based on the number of modules and features included for Basic Users in the State's DLAN system as well as the group size. BCG will run multiple basic user training course sessions over a two-day period to accommodate larger audiences and ensure all staff is trained. Users only need to attend one session.

5. *Schedule for standard yearly training course.*

BCG can provide DLAN Refresher Training on a yearly basis. Refresher Training consists of condensed versions of the administrator, advanced, and basic user training courses as well as coverage of new features and functionality introduced over the last year with DLAN system updates. If annual onsite instructor led training is not the best approach for the State based on the number of users to be trained or their geographic dispersal, BCG can provide an alternative solution such as online webinar or video based training as a yearly refresher course. For several clients, BCG also develops and runs tabletop or full scale exercises annually as part of their refresher training.

6. *Type of course material that will be provided (course handouts, presentations, and other training materials).*

- DLAN Training Agenda (Training Plan) for Basic User Course, Advanced User Course, and Administrator Course.
- DLAN Quick Reference Guide Documents (Training Materials) for Basic User Course, Intermediate User Course, and Administrator Course.

- DLAN Training Course PowerPoints or Recorded Video of Trainings for Basic User Course, Intermediate User Course, and Administrator Course.

6. *Methods of ongoing, continuing, and on demand training.*

Online Help – The DLAN system includes a built-in online help system that features approximately 375 articles that cover all aspects of the software’s use and functionality with text, images, and step by step instructions. The help system is context sensitive, ensuring that when a user clicks the help button he or she is directed to a relevant article based on the feature or page with which the user was interacting. The help system works with both an online and offline connection. The help system serves as a real-time updated user manual and fosters self-paced learning and as a training refresher on system functionality.

In addition, BCG Support’s Help Desk is available 24/7 and BCG will provide two days of onsite instructor-led DLAN refresher training per year. And you can also schedule new release review webinars on demand with knowledgeable BCG Test Engineers and QA staff.

4.2.1.1.10 *The Vendor shall provide initial training on-site for the following users. This training must be accompanied by user manuals.*

1. *System Administrators to include user access management, a minimum of ten (10) users.*

BCG will provide 2 days of onsite instructor led system administrator course training. BCG will provide administrator training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

2. *State Agency representatives, a minimum of fifty (50) users.*

BCG will provide 2 day of onsite instructor led advanced user course training for state agency representatives. BCG will provide advanced user course training documentation in the form of quick reference guides. Documentation will be delivered electronically.

3. *Local Jurisdiction representatives, a minimum of two hundred (200) users.*

BCG will provide up to 4 total days (shared with NGO training) of onsite instructor led basic user course training for local jurisdictions and NGOs. The days of training will be broken up into multiple sessions. Users will only need to attend one session. Session length is variable based on the number of users to attend, but is typically 4-8 hours depending on group size and the configuration of the state’s DLAN site. This training will be shared between Local Jurisdictions, NGOs, and break-out sessions for technical staff who are expected to have a similar level of access. BCG will provide basic user training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

4. *Non-governmental Organization Representatives, a minimum of one hundred (100) users.*

BCG will provide up to 4 total days (shared with Local Jurisdiction training) of onsite instructor led basic user course training for NGOs and local jurisdictions. The days of training will be broken up into multiple sessions. Users will only need to attend one session. Session length is variable based on the number of users to attend, but is typically 4-8 hours depending on group size and the configuration of the state’s DLAN site. This training

will be shared between Local Jurisdictions, NGOs, and break-out sessions for technical staff who are expected to have a similar level of access. BCG will provide basic user training course documentation in the form of quick reference guides. Documentation will be delivered electronically.

5. *Federal Agency Representatives, a minimum of twenty-five (25) users.*

BCG will provide a tutorial Video-based training course for Federal Agency Reps that is designed to provide a self-paced learning path for Federal Reps. Documentation will be delivered electronically. These users are expected to have an observer level of access and should need limited training. However, Federal Reps who need or desire a higher level of access can attend the basic user training course.

4.2.1.1.11 *Document Management. The EMIS shall offer a document management component to support the emergency management workflow.*

The DLAN Reference Library and Incident Folders Modules provide document management features for users and administrators.

Reference Library- The Reference Library is DLAN's main file storage area and is designed to make files and documents available to staff anytime, anywhere. It is included with our DLAN Advanced and Premium editions and can be added to any DLAN System. Unlike DLAN's other file storage area, Incident Folders, the Reference Library is not incident specific and is designed to store persistent data that needs to be accessible for all incidents, such as policies, procedures, and emergency evacuation plans. Three features that differentiate DLAN's Reference Library from other file storage applications are that it is fully accessible from mobile devices; its intuitive security settings allow folders to be locked down by security group to protect sensitive information; and that it can be used to upload any type of file (unless specifically prohibited by an administrator).

Incident Folders- The Incident Folders include all of the features of the Reference Library, but is designed to save incident specific documentation, such as disaster scene photos, press releases, news articles, agency generated documents, reports, and ticket information. With Incident Folders, each incident has its own set of incident folders. The structure of these folders can be pre-defined to create a consistent organizational structure for saving incident specific files. Like the Reference Library, security can be set for each individual folder, so that only authorized security groups will have access to the information. Other DLAN modules have quick-links to add items to Incident Folders and items in the Incident Folder can also be posted to other modules, such as the Status Board. At the end of the Incident, all materials stored in Incident Folders can be downloaded, rolled into a report, or Emailed out. Incident Folders are included with our DLAN Advanced and Premium editions and can be added to any DLAN System

1. *The EMIS shall enable users to access procedures, check lists and organization charts, and other documents.*

DLAN's Reference Library provides easy access to plans, procedures, checklists, organization charts, and other documents. Documents stored in the Library can be shared, secured (visible only to authorized users), and posted

to dashboard as needed. Additionally, the DLAN Incident Action Plan & ICS Forms module support the ICS 207 organization chart form which can be filled out saved, shared, and posted.

2. *The EMIS must allow users to import and export information including resource data.*

DLAN allow users to import and export information such as resource data through standard tools. Resource data as well as any other data tables can be exported using the export button (CSV, Excel, Word, PDF, etc.). Reports and documents can be shared via email and other methods to internal users or external sources. Files such as GIS files can be downloaded as KML, Shape, or CSV files.

3. *The EMIS shall enable users to prepare and disseminate situation assessment information and recommendations.*

DLAN allows users to prepare and disseminate situation assessment information and recommendations to both internal and external stakeholders through the Situation Report module. Agency Reports can be submitted by the roles responsible, the Situation Report document can be compiled by the planning section or a relevant position. Finally, the individual reports or the Sit Rep can be viewed in DLAN, forwarded out to stakeholders via email, or posted to a Dashboard for consumption as situational awareness information.

4. *The EMIS shall provide access to electronic West Virginia Emergency Operations Plan, State Emergency Operations Center (SEOC) Standard Operating Guidelines (SOG), Incident Command System (ICS) forms, documents, and templates for approved user to edit, update and subsequently store within the application in the user interface.*

DLAN will allow approved users to edit, update, and store documents and templates within the Reference Library Module of the system. Please see (4.2.1.1.11) for more information on this module.

5. *The system must also provide for customization of displays or reports, based on the users' needs*

DLAN is a highly configurable system designed to make filtering of data easy for users. There are numerous ways that customized views, dashboards, landing pages, status boards, and reports can be created on the system. The following are just a sampling of the many ways that displays and views can be customized by users:

- **User, Role, and Task Based Status Boards** – Customized views can be created out of any of the modules and situational awareness panels on the system to allow for user, role, and task specific views to be created and re-used on the system. These dashboards can also be set as a user's or role's landing page (homepage) in the DLAN system. Combined with Workflow Mappings, this presents a completely tailored user experience for each federal or state agency, local jurisdiction, NGO or other organization on the system.
- **Customizable Ticket Reports** – In the Ticket Manager, ticket reports are used to filter the list of available tickets down into meaningful sets of similar tickets so that they can be more easily tracked, worked upon, and completed. Customized views of ticket data (reports, requests, donations, etc.) can easily be queried based on date time range, incidents, priority settings, status settings, jurisdiction data, user submission data, location data, routing information, keywords, attachment data, and other information. Users can select the columns they wish to see in the report, using any data within the ticket or any dynamic forms created for or by WV staff (i.e. damage assessments, debris clearance forms, sheltering forms, etc.). These queries can easily be saved for use by other groups of users in map reports, in ticket manager grids, in

status boards, and as personal reports. This ability to quickly filter and present data for temporary or permanent use allows the Ticket Manager to be a core data management system for customer displays and views on the system.

- **Customizable Phone Book Reports** – Like the ticket reporting tools, phone book data can easily be filtered by users to display organizations and people based on filterable criteria such as location, trainings completed, skills possessed, categories, text, and other filters. These reports can then be saved for use by other users on the system in order to easily find contact information on vendors and staff that is specific to require emergency management needs.
- **Filterable Grids** – Every table of data on DLAN includes filters to find textual data within the grid. Additionally, many grids include advanced filtering capabilities such as date/time ranges, category filters, location filters, routing filters, active/de-active data filters, organization filters, status filters, and other types of filters. Additionally, any grid is re-sortable by clicking on the headers of a particular column. These advanced capabilities make it easy for any table of data on DLAN to be filtered as per the needs of the users.
- **Map Reports** - In addition to the dashboard, landing pages, and situational awareness views that users can create, Map Reports can be used to display specific map information. GIS administrators can configure map reports including basemap and layer settings to be viewed in the COP Viewer or as part of the Status Board.

6. The EMIS must generate reports as requested on the levels of material at the report time and usage or consumption over a defined time interval to enable consumption to be addressed.

The DLAN Resources Module provides a view of all resources used during the incident. It can be searched or filtered by NIMS Type, Category, or Location. The Resources Module provides several standard reports that can be generated as needed. These include a master resources inventory list, detailed organization resource inventory list, and summary organization resource inventory list. User can track material levels, usage, and stockpile levels for each resource kind.

7. The EMIS must be able to receive, record and log incident intelligence and security reports from identified and verified external agencies

DLAN can log intelligence and security reports from external agencies through the use of the DLAN Mobile Responder App. External Agencies can use the app to submit an incident intelligence report, security report, or any other type of information. This information is filled out on the app using customizable forms. When saved, the data is synchronized to DLAN in real time and populates a Status Board with the relevant information. It can also populate tickets and trigger notifications and alerts.

8. The EMIS shall be capable of storing and managing documentation to be retained as record.

DLAN is an audit ready system that automatically logs all historical data. In addition to retaining official documentation, DLAN will allow administrators to run incident reports. Incident reports are comprehensive chronological reports detailing all additions and modifications to records and data that occurred during an incident or event. Reports can be filtered down to a specific date range or type of records, including tickets, messages, broadcasts, Status Board items, uploaded Incident Folder Documents, Situation Reports, ICS Forms, Incident Action Plans, and GIS Map Snapshots. Like other DLAN reports, the Incident Report can be exported or printed as needed.

9. *All data shall remain the property of the state and will not be available for dissemination by the vendor.*

All data entered into DLAN will remain the property of West Virginia and will not be disseminated by BCG.

4.2.1.1.12 *Logistics support. Resource management. The EMIS shall enable users to direct, task, receive, and monitor resource requests.*

DLAN's robust Ticket Manager System and the integrated Resource Request functionality provides concise logistical support within the system. It allows users to direct, task, receive, and monitor resource requests.

Standard Resource Request - The Resource Database is DLAN's main resource inventory portal. It provides a way to enter, manage, and track supplies and resources. Resources can be added to organization records to establish suppliers and inventory stockpiles. They can also be automatically matched to tickets in the Ticket Manager making fulfilling resource requests quick and easy. As resources are added to the resources stockpile or deployed for use during an incident, the list of available resources can be updated accordingly, giving an accurate, real time listing of available resources. It is included with our DLAN Advanced and Premium editions and can be added to any DLAN System. Tickets with resource requests can be routed to specific users for fulfillment.

Standard Resource Forms and Reports include: Request form, and Field report forms.

The Ticket Manager is DLAN's main resource, issue, resource and task management module and is included in all our standard editions. It creates a common area for collaborative issue tracking, initial resource requesting and real-time information sharing using straightforward color-coded statuses and priorities. The Ticket Manager provides user-friendly data entry tools to make logging and tracking critical information quick and easy. It allows both task and mission information to be entered, prioritized, routed/assigned, and followed from start to completion. The Ticket Manager includes preconfigured forms for capturing additional resource request information and capturing information from off-site-staff. It also includes preconfigured reports for easy access to essential information. Additional forms and reports can be purchased individually, or you can upgrade to Ticket Manager Premium to gain access to DLAN's custom report builder.

1. *The EMIS shall enable users to plan and manage the acquisition and distribution of personnel, equipment, and material required to sustain an incident operation.*

Logistics support users can triage and manage resource requests, personnel requests, acquisitions, equipment and other materials related to an incident. The Find Match button allows them to match up a request ticket with a stockpile resource or vendor. The Assets Module, allows logistics support users to track equipment assigned to the field including its current location and status (e.g. en-route, on-location, ready for demobilization, etc.). This type of logistics function is an area where DLAN truly excels above other EMIS software through its Ticket Manager, Resources, and Assets functionality.

2. *The EMIS shall enable users to register, update, and delete resources from the resource management component.*

DLAN's resources module functionally allows users to register, update, and delete resources from the resource stockpile and management ledger as needed. The ability to do so is security controlled based on permissions.

Additionally, users can request, update, and offer resources through the Ticket Manager's resource request and management features.

3. The EMIS shall offer a resource request option with the capacity to document partially fulfilled requests.

The Resource Request tickets entered into the system by users can be routed (assigned/shared) to one or more roles or positions. Multiple users, liaisons, and other contributors can partially or fully fulfill the request. Resource request questions and additional information can be collected on the request form and notes from participating agencies, liaisons, and users are tracked in the log notes. Once resources or equipment are deployed to the field the assets tab of the ticket tracks the individual fulfillment, status, and location of each resource individually as a sub-component of the request ticket.

4. The EMIS shall enable users to track the pre-positioning of resources and managing supplies in facilities.

The DLAN Phonebook allows logistics support users to build out vendor, organization, and facility records including what resources are owned by that organization or currently located at that facility. This is especially useful when setting up staging areas and forward command posts. These records can be populated ahead of time and displayed on the DLAN GIS Map for geospatial planning and analysis.

5. The EMIS shall enable users to task transportation resources to transport and deliver supplies.

The DLAN Ticket Manager module is designed to allow users to task out responsibility for an action to another role. Logistics users can receive a resource request ticket, source the equipment, and then route the ticket forward to a transportation role for delivery of the supplies. Each role plays their part in completing the ticket. At each stage notes and actions are logged, the ticket status is updated to reflect its current spot in the process, and users are alerted when a new ticket lands on their dashboard or report.

6. The EMIS shall enable users to monitor and forecast the consumption of supplies.

The DLAN Resources Module allows logistics users to decrement known stockpile resources as they are consumed so that additional supplies can be sourced when stocks get low. Additionally, the Statistics feature allows user to view resource request tickets broken out by type, kind, role responsible, and other trends so that users can forecast future supply needs.

7. The EMIS must allow users to plan, manage, track, and observe costs incurred.

The DLAN Finance Module provides the necessary tools to help users and administrators track costs for missions, tasks, and resources. It is based on FEMA's reporting standards and can also be configured to the state's needs. Finance records can be entered either from the finance tab in a ticket or through the Incident Ledger page. Each finance item is associated with a particular incident and with a ticket that tracks the finance request and its current status. DLAN comes pre-loaded with a resource list and cost codes that are based upon FEMA's equipment list costs. Custom resource codes and costs can also be added by an administrator. Information about the item, delivery info, wage info, and invoicing are all recorded by the system.

8. The EMIS shall provide users electronic and printable forms for logging and reporting the ordering, receiving, and issuance of material.

Asset Tracking provides a way for users to track deployed assets and resources for a particular incident and quickly view the status, quantity, and location of all deployed assets in the asset ledger. All forms and reports can be printed.

The screenshot shows a web form titled "Edit Asset". The form has the following fields and values:

- Item: Snow Blower (8580) - 2,000 tph - 400HP
- Description/Notes: Small Snow Blower
- Serial Number: 321654987
- Quantity: 3
- Resource Provider: International Relief
- Obtained: Stockpile
- Transporter: Highway Department
- Status: On Scene / Deployed (highlighted in red)
- Ticket ID: 3182-3178 - Move snow at high school
- Label: (empty)
- Location: Lat N42°47'45.77" Lon W78°50'41.39" (with a location pin icon and a green checkmark)

Below the Location field, it says "Geocoded as: POINT(-78.84483 42.796048)". At the bottom right of the form are three buttons: "Save", "Delete", and "Cancel".

Figure 15: Asset Form

9. The EMIS shall receive, log and report to users the status of personnel, equipment, and logistics resources throughout an event.

Reports can be created within the system and made accessible by authorized users/teams on the real time status of all resources throughout an event. This feature is included in the Ticket Manager Premium Module. Once created, a report can be added to a Status Board for visual display and sharing.

10. The EMIS must enable logistics support users to plan and monitor the routing and movement of supplies from staging areas, distribution points, and other supply facilities.

DLAN supports supply chain logistics and transit of vehicles, equipment and supplies through the use of the Assets and GIS Modules. Logistics support users can plan a route on the map, mark it up, and share it with other agencies or parties as a static map image, interactive map report, or as a downloadable KML file. If West Virginia has GPS tracking devices that they use on their equipment or vehicles (ex: magnetic slap and track devices), those can be integrated and displayed on the GIS Map. The DLAN Mobile Responder App can also be used as a GPS tracking device. This allows vehicle operators transporting supplies to download the app (free from the app store) and they can be tracked in real time in DLAN.

11. *The EMIS must enable logistics support users to monitor and manage stocking levels of supplies held in staging areas, distribution points, and other supply facilities.*

The DLAN Resources Module is designed to allow users to pre-populate DLAN with known supplies and resources along with their location and contact person/ordering information into a known "Stockpile." Each supply depot facility can also be entered into DLAN as a record and displayed in resource reports, phonebook contact reports, and on the DLAN GIS Map. This provides three ways to monitor and manage stocking levels. Additionally, the Resources Module allows users to decrement and track quantity, cost, and other basic supply information.

12. *The EMIS must be capable of allowing accessibility on mobile devices in an application format. Mobile applications shall be able to perform all functions of basic inventory management without the need for data connectivity due to potential lack of communications in remote sites. Mobile applications shall be able to perform automatic inventory updates when a user enters into an area that has data connectivity available.*

DLAN does have a mobile app that has versions for Apple, Android, and Windows devices. The Mobile app can be used to perform basic inventory management tasks without the need for data connectivity, and will automatically sync the data when a connection is available. For example, a user can submit a resource request from the field and have it sync to the system for management and fulfillment. Additionally, updates and assignments can be pushed from the web interface down to the individual mobile device of a user who is responsible for the information.

13. *The EMIS shall be capable of supporting hardware such as barcode/QR Code scanners and barcode/QR Code printers. Mobile applications shall be capable of utilizing the mobile device camera as a barcode/QR Code scanner.*

The EMIS is capable of supporting hardware such as barcode/QR Code scanners and printers. For example, DLAN users can add QR codes to Status Boards and documents that can then be scanned using a phone or device to prompt an action such as accessing an executive summary report, linking to other sites for additional information or briefings, etc. Mobile devices can scan bar codes or QR codes using the camera on the mobile device. Images of Bar codes and QR codes can be captured using the app and attached to submissions.

4.2.1.1.13 *Financial and administrative support. The EMIS shall provide support for the following processes:*

4.2.1.17.1. *Identify material and personnel that require payment.*

The finance tab in a DLAN ticket can be used track the material, personnel and required payments associate with a finance cost. The ticket's statues can be used to track payment progress and can be adjusted as a cost moves through the system. For example, the ticket status may be set to Procurement Needed, Approved, Payment Pending, Paid, Reimbursement Pending, etc. These statuses are configurable by a system administrator.

The DLAN Incident Ledger page also provides data for reimbursement payments including 25% and 75% reimbursement rates and total sums.

4.2.1.17.2. Enter and record all cost data.

The DLAN Finance Module does allow users to enter cost data, and that data will be saved and easily accessible.

4.2.1.17.3. Maintain accurate records of incident costs.

The DLAN Finance Module's Incident Ledger feature allows users to quickly generate custom reports about financial items for the current incident. All finance pages support searchable and sortable data columns, exporting data to Excel, Word, or CSV files, and automatic subtotaling and totaling sums. This means that the current spend level for the incident is always totaled and available.

4.2.1.17.4. Support planning activities through preparation of estimates for resource usage.

DLAN supports planning activities including the preparation of estimates and expected resource usage through the use of the Preparedness Toolkit features. This functionality allows an authorized user or administrator to prepare templated tickets ahead of time for common resource requests and standard mutual aid requests such as mission ready packages. These templated tickets can include all financial information and costs relevant to equipment and personnel involved with the task or mission. Templated tickets can be activated individually or in bulk (mass activated) by an administrator as needed. Templates can also be used by basic users as a way to enter a standardized ticket with pre-filled information in a quickly and accurately rather than building a resource request ticket from scratch. Finally, templated tickets are associated with a scenario/incident category and can be automatically activated when an incident of that type is created. This provides an immediate action plan and important tasks at the beginning of an incident response when time is most critical.

1. Financial and administrative support for procurement of material and services.

The Finance Module provides all necessary information to track procurements, purchase orders, receipts, and payment information for materials and services. Finance information is viewable in a tabular page or on a dashboard or mobile device.

2. Monitoring and reporting of costs related to an incident.

All costs associated with an incident are tracked in the Finance Module. This includes individual line items for resources, equipment, personnel, and services with quantity, unit costs, and expected total costs. The Finance Incident Ledger also automatically totals all running costs for the incident so that the State knows when their obligations are met and when federal will become available. The Finance Module also allows finance users to create configurable reports to get detailed information on specific resource types, categories, purchase orders (with multiple items), vendors, statuses, date filters, and DRP eligibility.

3. Providing cost analysis services.

DLAN's Finance Module is designed to track all costs and display running totals for each task, mission, and the incident as a whole. Customizable finance reports help with analyzing trends. DLAN also tracks displays promised payments, payable by, and expected costs as well as delivery,

wage info (normal/overtime), and invoicing information. With all this information in the system, the backup data for reimbursement is simple and at the state's fingertips.

4. *Documenting individual transaction receipts.*

DLAN's Finance Module does save all transaction history, no matter how small.

5. *The EMIS must enable users to provide administrative support for procurement of materials and services including the ability to:*

1. *Identify local sources for equipment rentals.*

The Find Match feature in the DLAN ticket matches a resource request entered by a user with a known supplier of that type of resource. It matches a request ticket with a resource record and phonebook contact for the supplier. This includes equipment rental services.

2. *Identify local sources for material supplies.*

The DLAN Resources Module is designed to track suppliers and supplies of equipment. Users can view contact persons, location, purchasing information, cost, and quantities for equipment rentals.

3. *Record orders and receipts for equipment and supplies.*

All orders and receipts for equipment and supplies can be tracked within a DLAN Ticket. The Ticket serves as a central place that aggregates all information related to a task, from the initial resource request, through logistics, procurement, resource deployment, demobilization, and finance recovery. Orders and receipts for equipment and supplies can be uploaded to the ticket as an attachment.

4. *Provide capability for the upload/import of database of existing or acquired inventories.*

As part of WV's project implementation, BCG will import a database of existing or acquired inventories into DLAN. This is typically achieved through the upload of an excel or CSV file of data. BCG can provide a recommended import template for resources. After initial implementation, WV's DLAN maintenance and support plan entitles the state to several imports or refreshes per year to maintain the data.

6. *The EMIS must enable users to provide cost analysis services including the ability to:*

1. *Identify material and personnel that require payment.*

The finance tab in a DLAN ticket can be used to track the material, personnel, and required payments associated with a finance cost. The ticket's statuses can be used to track payment progress and can be adjusted as a cost moves through the system. For example, the ticket status may be set to Procurement Needed, Approved, Payment Pending, Paid, Reimbursement Pending, etc. These statuses are configurable by a system administrator.

The DLAN Incident Ledger page also provides data for reimbursement payments including 25% and 75% reimbursement rates and total sums.

2. *Enter and record all cost data.*

The DLAN Finance Module provides the necessary tools to help users and administrators track costs for missions, tasks, and resources. It is based on FEMA's reporting standards and can also be configured to the state's needs. Finance records can be entered either from the finance tab in a ticket or through the Incident Ledger page. Each finance item is associated with a particular incident and with a ticket that tracks the finance request and its current status. DLAN comes pre-loaded with a resource list and cost codes that are based upon FEMA's equipment list costs. Custom resource codes and costs can also be added by an administrator. Information about the item, delivery info, wage info, and invoicing are all recorded by the system.

3. *Maintain accurate records of incident costs.*

The DLAN Finance Module's Incident Ledger feature allows users to quickly generate custom reports about financial items for the current incident. All finance pages support searchable and sortable data columns, exporting data to Excel, Word, or CSV files, and automatic subtotaling and totaling sums. This means that the current spend level for the incident is always totaled and available.

4. *Support planning activities through preparation of estimates for resource usage.*

DLAN supports planning activities including the preparation of estimates and expected resource usage through the use of the Preparedness Toolkit features. This functionality allows an authorized user or administrator to prepare templated tickets ahead of time for common resource requests and standard mutual aid requests such as mission ready packages. These templated tickets can include all finance information and costs relevant to equipment and personnel involved with the task or mission. Templated tickets can be activated individually or in bulk (mass activated) by an administrator as needed. Templates can also be used by basic users as a way to enter a standardized ticket with pre-filled information in a quick and accurate manner rather than building a resource request ticket from scratch. Finally, templated tickets are associated with a scenario / incident category and can be automatically activated when an incident of that type is created. This provides an immediate action plan and important tasks at the beginning of an incident response when time is most critical.

4.2.1.1.14 *Forms and templates. The EMIS shall provide the electronic fillable and printable forms for users to prepare, share, present, electronically sign, and print required documents.*

DLAN allows administrators or authorized users to design, build, and deploy custom fillable forms such as a contingency operations plan. Forms can include fields, tables, drop-down lists, text, images, and other attributes as well as electronic signature capture fields. DLAN can also track dates and times for a form field, for example automatically record when a form is signed. This can be used to trigger workflows or build in automation. All forms

created in DLAN can be deployed to the Mobile App for users in the field or at other locations to fill out forms and sync the data back to the DLAN system where it can be displayed on a report or dashboard and then managed accordingly as either a ticket or an assessment.

1. The EMIS shall enable electronic and customizable forms.

DLAN provides electronic forms that can be created, customized, and updated by authorized users. Once created, the forms can be used with the resource request process, assessment process, role checklist process, the GIS map, ArcGIS, reporting, templates, the mobile app, and more.

2. The EMIS shall allow users to update, create or import user generated forms. System upgrades must allow for continued use of previously generated forms.

Users in DLAN have the ability to create custom forms within the system using a simple no-code WYSIWYG style form builder tool. Existing web forms can be imported into the system by copying and pasting the html of the form into the DLAN EMIS form builder tool. Forms in other formats such as a MS Word document can be saved as a web page and then opened with notepad to copy and paste the contents into the EMIS to import the form.

System upgrades do not affect the ability to use previously generated forms. Updating a form layout with new fields or information will not impact historical records with the old version of the form, only newly created entries going forward. Or, administrators can choose to override and update old instances of the form to the new version.

4.2.1.1.15 Situational Awareness. The EMIS shall be able to provide tailored views.

Customized views can be created out of any of the modules and situational awareness panels on the system to allow for user, role, and task specific views to be created and re-used. These dashboards can also be set as a user's or role's landing page (homepage) in the DLAN system. Combined with Workflow Mappings, this presents a completely tailored user experience for each federal or state agency, local jurisdiction, NGO or any other organizations on the system.

1. The EMIS's situation display shall be able to display geographical views with geo-referenced features on map overlays.

DLAN's GIS Premium module provides geographical views of selected areas and allows users to activate map layers that appear in real time with accurate geo-referenced data.

2. The EMIS's situation display shall be capable of displaying one or more selectable map overlays.

Map Reports can be used to display specific map information. GIS administrators can configure map reports including basemap and layer settings to be viewed in the GIS display or as part of a status board. They can also display multiple map overlays and seamlessly integrate said layers into the map in real time.

DLAN's GIS Premium module allows for multiple map overlays to be activated at once and shown on the Legend column.

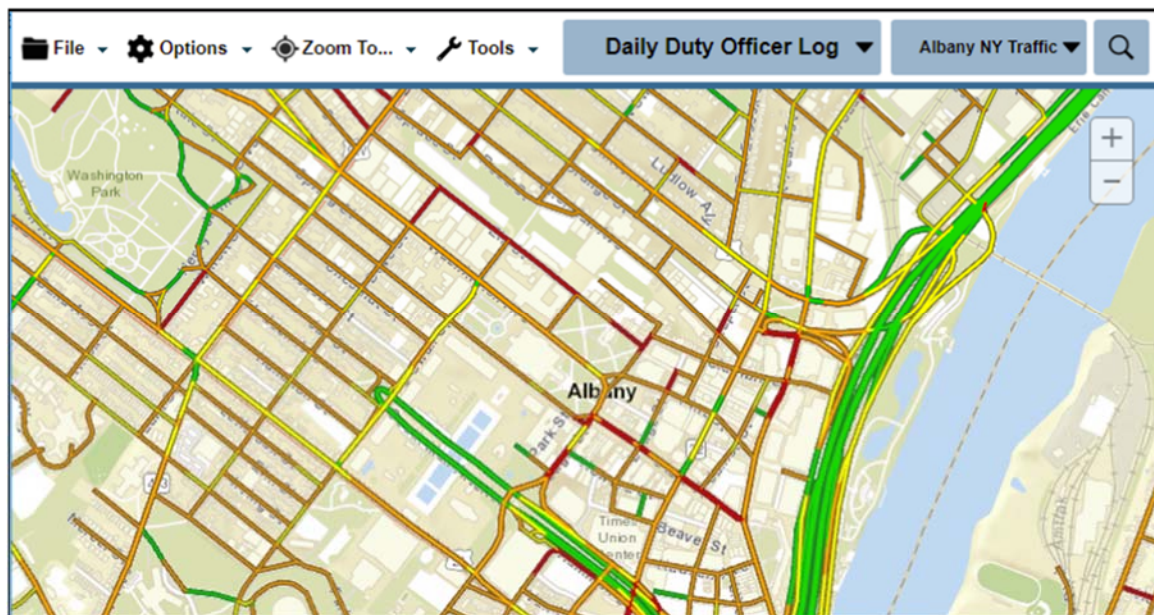


Figure 16: Map Report - Traffic

3. *The EMIS's situation display shall be capable of displaying a situation report, operational information, status report, or map image received from users.*

DLAN's Status Boards can display any information from within DLAN and from multiple external sources, including situation reports, operational information, status reports, or map images received from users.

4. *The EMIS's situation display shall include the ability to display selectable levels of detail to enable users to see summaries such as a dashboard display to indicate elements that may require attention.*

The DLAN Status Boards (dashboards) allow both overview and macro views of incident status information and detailed status information on roles, teams, tasks, and critical incident messages. Status Boards update automatically in real-time as new information is entered.

Several tools are available on the Status Board to help users drill down to key status information including the Stats page which shows statistics based on role and task; Ticket Reports, which show individual tasks and their completeness; and incident messages, which allow users to post situational awareness information or critical decisions.

5. *The EMIS's situation display shall be capable of integrating and displaying live images and audio/video feeds from external sources such as traffic monitors, security cameras, surveillance cameras or data feeds.*

Streaming Video allows you to access any IP-based video feed, including streaming and snapshot cameras, for improved situational awareness. Video streams can be chosen using an easy drop-down menu and displayed simultaneously on the Streaming Video dashboard or be popped out into their own windows

for enhanced viewing. Live images and audio/video feeds can also be displayed directly on the GIS Premium map.



Figure 17: Streaming Video on Map

6. *The EMIS shall be capable of capturing and disseminating the image showing on the situation display to selected user(s).*

Images can be shared within the system to selected users by controlling who has access to a board or image file. Images from the situation display can also be shared internally or externally via message or email.

7. *The EMIS shall provide for managing and reporting of injuries and deaths.*

The system can provide a way to report on injuries and deaths and manage that information through the use of secure tickets. A secure ticket is locked so that the sensitive information contained inside is only visible to roles that have been specifically routed the ticket (shared with them). Secure tickets can be collated in a Ticket Report designed to capture and display that information on a Status Board. Both the report and the board can also be secured so that only specific users get access to them.

4.2.1.1.16 *Community Lifelines. The EMIS shall automatically generate a dashboard, and status based on the Community Lifelines. The EMIS shall allow users to generate and store time-stamped Community Lifelines reports based on jurisdiction and event.*

The DLAN system includes a Community Lifelines toolkit designed to assist users with managing lifeline information and reports. Status Board (dashboard). The toolkit consists of a Community Lifelines data collection form that can be filled out from either the web interface or from the mobile app. The data submitted on the form automatically populates a Community Lifelines Report that displays detailed and critical information. The report is then displayed in a dynamic GIS Map and Dashboard with color coding for condition and trend on each event as well as other critical information. This overall workflow allows users to create lifeline reports for all of FEMA's seven community lifelines (Safety and Security; Health and Medical; Communications; Hazardous Materials; Food, Water, Shelter; Energy (Power & Fuel); and Transportation.). The result is time stamped and accurate reports that are filterable by lifeline, jurisdiction, and event kind that provide a way to make better informed emergency decisions.

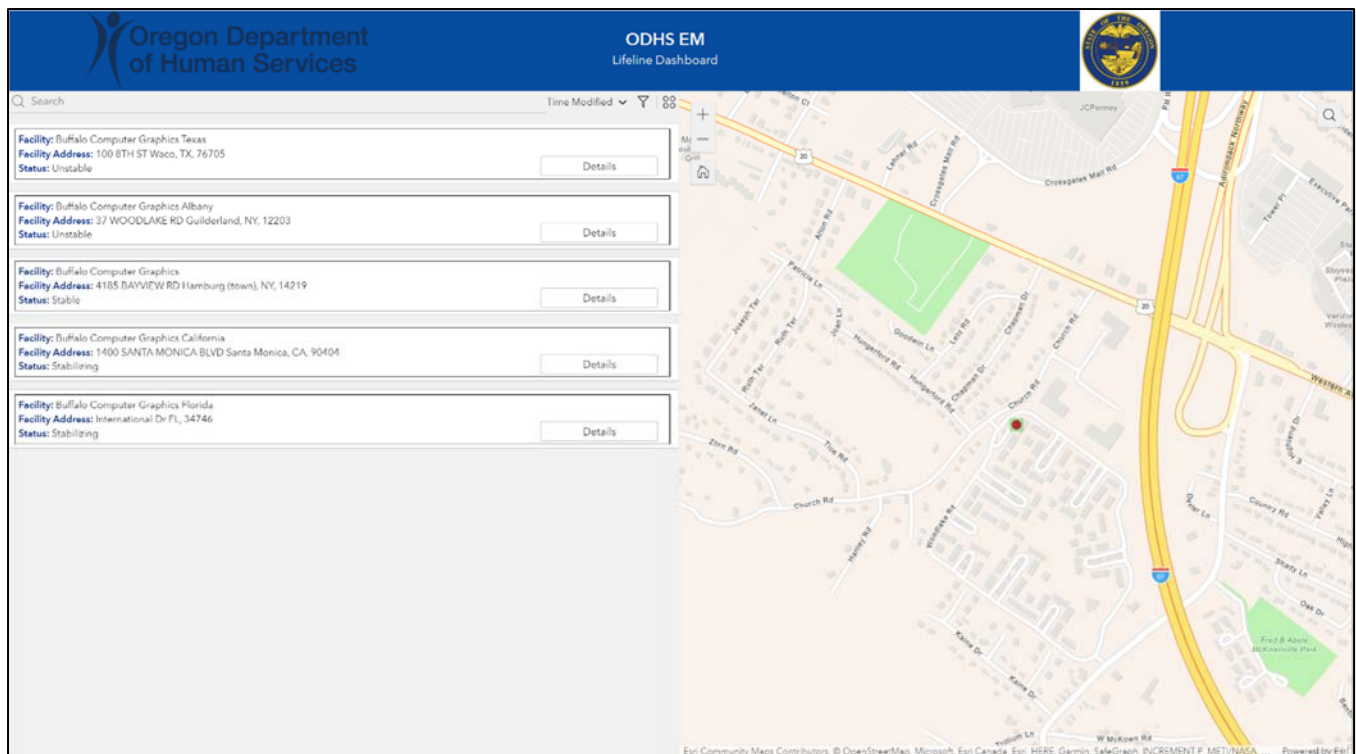


Figure 18: Community Lifelines Dashboard

4.2.1.1.17 *Communication. The EMIS shall offer chat rooms and virtual conference rooms configurable by users. The EMIS shall enable the users to capture and manage content. The EMIS shall enable the users to save and store documents, recordings, and aids used in a chat room or virtual meeting.*

The Chat Module is DLAN’s internal instant messaging system and is included with all systems. It can be used to send and receive user-to-user messages. When sending a chat, the system will display other users that are online as well as their role (function) to make finding the correct person simple. All chat history is saved and can be viewed by the participants as well as by an administrator with advanced permissions. This means that any documents, recordings, or aids will be saved and accessible. Users can also initiate chat rooms for multiple participants. Chat rooms can be initiated independently or from within a ticket and saved as part of the ticket log, eliminating the need for duplicate data entry and creating a more complete record of decisions.

1. *The EMIS must provide the means to communicate easily with one or more remote users (by name or by function) using real time text messaging that is logged and recorded.*

Using the Chat Module, DLAN allows users to send messages to other users on a one-on-one basis or in a group in real time. All chat history is saved and can be viewed by participants as well as by an administrator with advanced permissions.

2. *The EMIS must have the ability to send automated text messages, voice chat messages, or video messages to mobile devices.*

DLAN can send automated or manually triggered text messages, voice phone calls, and emails to landlines, mobile phones, and users' devices. This includes voice only capable devices. DLAN provides automated text and email messaging when an incident is created, when a situation report is due, and when a user is offline but a ticket has been routed to his or her role. Any messages sent to the device that is voice only capable will be handled by the device's native operating system.

3. The EMIS shall be capable of logging chat history in order to be retrieved by users at a later time.

All chat history is saved and can be viewed by participants afterwards in the Communication Center module. Chat history can also be accessed by an administrator with advanced permissions for audit or review purposes.

4.2.1.2 Software Administration. The EMIS's administrative and management functions shall be available to the system administrators.

System administrators have access to a large number of administrative and management functions within the DLAN software and the system is fully self-administrable by the client. A Full System Administration suite allows your administrators the ability to update and adapt the settings, preferences, lists, and values in real time as well as build their own dashboards and forms without needing vendor support and at no additional cost. Administration is available through the UI using simple tools, so no additional staff is needed to code or manage the system. This provides lower total cost of ownership over time.

With DLAN there is no need to use separate administrative menus for different areas of the system; universal system changes can be made from one easy to use menu. The System Administration menu includes three main categories: modules, system setup, and site security.

- Standard System Administration includes:
 - Site Security info: User, Group, and Role Management- The Site Security page can be used by administrators to create and manage user accounts, user/record level security groups, roles, and navigation menu links. Together these features allow the system to be customized to match a customer's workflow at no additional cost.
 - Module Administration settings- DLAN provides module administration pages can be used by administrators to change the configuration options for individual modules.
 - System Settings- The System Setup page can be used by administrators for configuration, presentation, and security settings that affect global DLAN system, not an individual module. For example, password security strength settings, login page graphics and text, and prohibited file type uploads.

4.2.1.2.1 The EMIS must provide user access through desktops, laptops, and mobile devices, such as, tablets or smart phones. The EMIS must let a user remain logged in at the same time on different devices.

DLAN is accessible through any web browser and also has a mobile app that works with Apple and Android phones and tablets. Additionally, a Windows app is available for use on desktops or laptops in addition to

accessing the site through the web-browser. A user can log into their account at the same time from both the web and on the mobile app.

4.2.1.2.2 *The EMIS must enable a user to sign on 'once' for access to all embedded applications.*

Single Sign-On can be implemented in DLAN. DLAN integrates with existing systems and includes single sign-on options for ease of use for users. The DLAN system tools allows for basic LDAP and Active Directory integration. It also includes tools for multi-factor authentication (MFA). Once a user is signed in they have access to all embedded applications.

Support for multiple simultaneous federated authentication / single-sign-on sources (as well as a hybrid model that supports both federated accounts for core users, and local user accounts for outside stakeholders and other agencies) DLAN supports federated authentication through Active Directory Federated Services accounts, SAML based accounts, and Active Directory (LDAP) based accounts. Any mix of these types of accounts can be utilized on the system at the same time.

DLAN's Single Sign On tools allow for Active Directory/SAML 2.0 based accounts to easily be utilized to setup default permissions, roles, access to content, access to data, and other settings within a user's account. The system also supports the use of multiple federations simultaneously so that a regional solution will support multiple organizations, each with its own active directory integration for provisioning and authenticating user accounts.

The following are available for Security Integrations:

- LDAP (outbound authentication)
- LDAP pre-registration (inbound user list synchronization)
- Federated Services (SAML 2.0, Shibboleth via ADFS)
- API based Integrations with Third Parties:
- Ticket Data API (two-way data sharing)
- EDXL-DE API (two-way data sharing)
- EDXL-CAP API (two-way data sharing)
- EDXL-HAVE API (inbound data sharing)
- EDXL-RM API (inbound data sharing)
- CAP API (two-way data sharing)

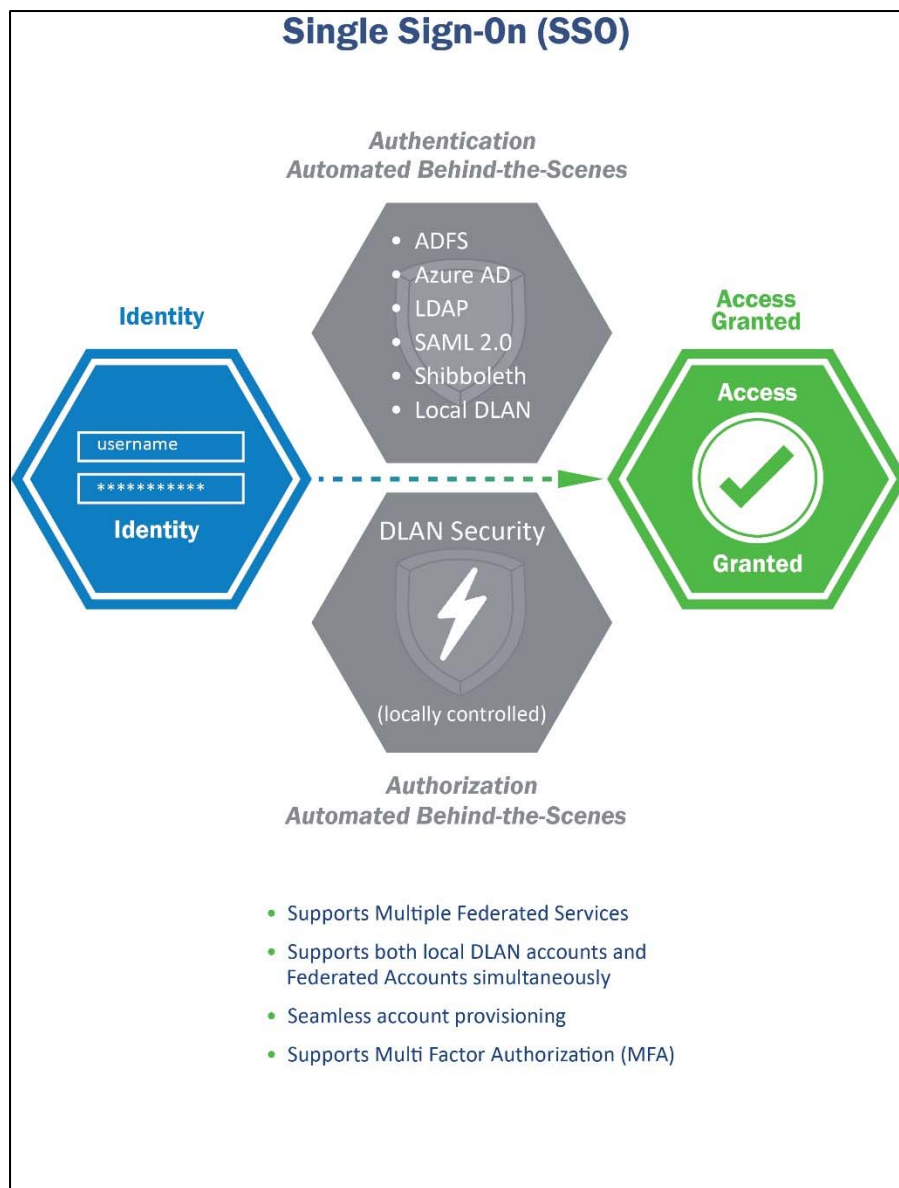


Figure 19: Single Sign On

4.2.1.2.3 *The EMIS shall be able to define a structured top-level organization with fully functional sub-organizations that operate in a hierarchy of authority.*

DLAN provides a structured top-level organization and fully functional sub-organizations through the use of its Record-Level data groups. These can be built-out as needed by a State System administrator. Users, permissions, and security can be assigned to the group.

4.2.1.3 Technical Requirements

4.2.1.3.1 *The EMIS shall be compatible with multiple factor identification and its use for system access.*

DLAN does not currently support multiple factor identification. This can be added as a customization; not included in proposal pricing.

4.2.1.3.2 The EMIS shall provide for single sign on and for PIV/PIV- I/CAC integration for system access based on Federal Information Processing Standard (FIPS 201-2) requirements.

<https://csrc.nist.gov/publications/detail/fips/201/2/final>

DLAN does not currently support single sign on through PIV/PIV-1/CAC. This can be added as a customization; not included in proposal pricing.

4.2.1.3.3 The EMIS shall record the failure of a login attempt. The solution shall have the flexibility to lock the user account after an Administrator-specified number of attempts. The solution shall have the capability of providing unattended password reset capability.

DLAN includes a security violations report that shows failed login attempts.

Username	Time	Resource	IP Address	Description
bog_cfire	3/19/2019 11:38:40 AM	jscoop.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /gis/jscoop.aspx?IsStatusboardMode=true&mapReportId=80 UserID (untrusted)= 1289 SessionUserId (untrusted) = 9881
bog_cfire	3/19/2019 11:38:39 AM	JSCOP.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /GIS/JSCOP.aspx UserID (untrusted)= 1289 SessionUserId (untrusted) = 9881
bog_cfire	3/19/2019 11:38:29 AM	SiteSecurity.aspx	[REDACTED]	User was booted from the system. theLogoutType = -1 User has cookie = True User accessing rawURL = /Admin/Security/SiteSecurity.aspx UserID (untrusted)= 1289 SessionUserId (untrusted) = 9880
mward	3/19/2019 9:10:10 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
mward	3/19/2019 9:10:09 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
mward	3/19/2019 9:09:58 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
bog_msaleh	1/8/2019 10:22:08 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
bog_msaleh	1/8/2019 10:22:08 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
cfire	10/30/2018 9:48:36 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination
cfire	10/30/2018 9:48:35 AM	Default.aspx	[REDACTED]	• Could not validate User Name / Password combination

Figure 20: System Administration - Security Violation Report

Administrators can specify the number of attempts before a user will be locked out in the Security Settings. The system also allows users to reset their password using a question and response method.

System Administration: Security Settings

Save Cancel

Enforce Strong Passwords: On Off

Passwords must be at least characters long

Passwords must contain at least lowercase character(s)

Passwords must contain at least UPPERCASE character(s)

Passwords must contain at least numeric character(s)

Passwords must contain at least special character(s)

Password Reuse

Users can reuse passwords

Prevent users from reusing the last passwords

Prevent users from reusing passwords

Bad Password User Locking: On Off

If user fails password attempts within minute(s), lock account for minute(s)

Require Phone on Login: Yes No

Require Role Selection on Login: Yes No

Allow Account Recovery: Yes No

Session Timeout in Minutes:

User Inactivity Logout Time (Minutes):

Duration to wait for answer (Seconds):

Mobile Responder App Timeout Window (Minutes):

Figure 21: System Administration - Security Settings

4.2.1.3.4 *The EMIS shall have the ability to provide event logging for successful logins, IP addresses of every authenticated user, failed login attempts, IP addresses of every failed login attempt, user database changes, log failures and/or errors.*

All of these report types listed here are available within DLAN’s System Administration.

4.2.1.3.5 *The EMIS shall include the means of recovering from a system failure using data previously backed-up.*

DLAN provides automatic recovery of data in several ways. First, all DLAN tickets have an auto-save feature that backs up a copy of the information the user has entered to their browser’s local cache. This means that if the user accidentally closes the ticket without saving, or loses connectivity, they can recover their draft to continue working.

At the technical level, DLAN services are resilient and will automatically self-restart if a service goes down or becomes unavailable. DLAN also supports load balanced servers, automatic or manual failover to another node, and a disaster recovery site.

4.2.1.3.6 *The EMIS shall limit access to those users who have valid login permissions and credentials.*

All users must have valid login permissions and credentials to access DLAN.

4.2.1.3.7 *The EMIS log in procedure shall include a requirement for users to agree to the state's confidentiality agreement prior to gaining access on each log in.*

DLAN includes a customizable User Agreement that be setup so each user has to click accept each time they log in. This agreement can either include the full text of the state’s confidentiality agreement or link to it, depending on the State’s preference.

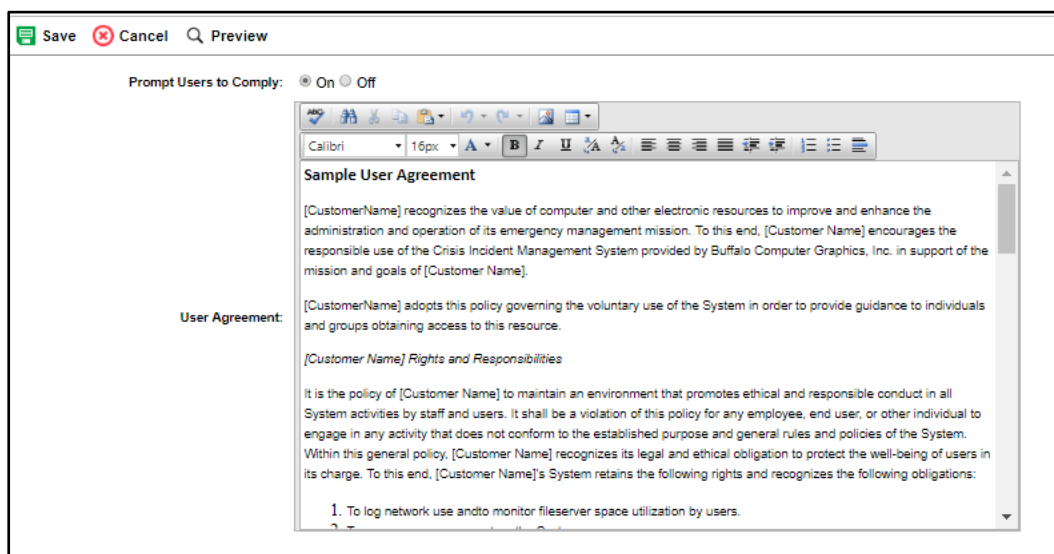


Figure 22: System Administration - User Agreement

4.2.1.3.8 The EMIS shall enforce strong alphanumeric passwords and periodic password changes. It means, minimum eight characters, combination of numbers, letters, special characters, and monthly password changes.

DLAN includes customizable password settings, please see Figure 21: System Administration - Security Settings on page 68.

4.2.1.3.9 The EMIS shall provide capability of a user to obtain password reset by administrator and by verification and via approved email and/or text.

Administrators can reset passwords either in bulk or individually. When a user's password is reset they are sent an email notification.

4.2.1.3.10 The EMIS shall be scalable to automatically accept any number of users to a maximum of 500 users logged in simultaneously with capability to add additional users with no delay.

The DLAN EMIS is scalable and can easily support up to 500 concurrent users logged into the system simultaneously. Additional users can be added on the fly and are not prohibited from accessing the system. Cloud hosting resources will be assigned to support the 500 user load and can be increased on demand by authorizing BCG support to do so. Please Figure 23: Scalability below for additional information.

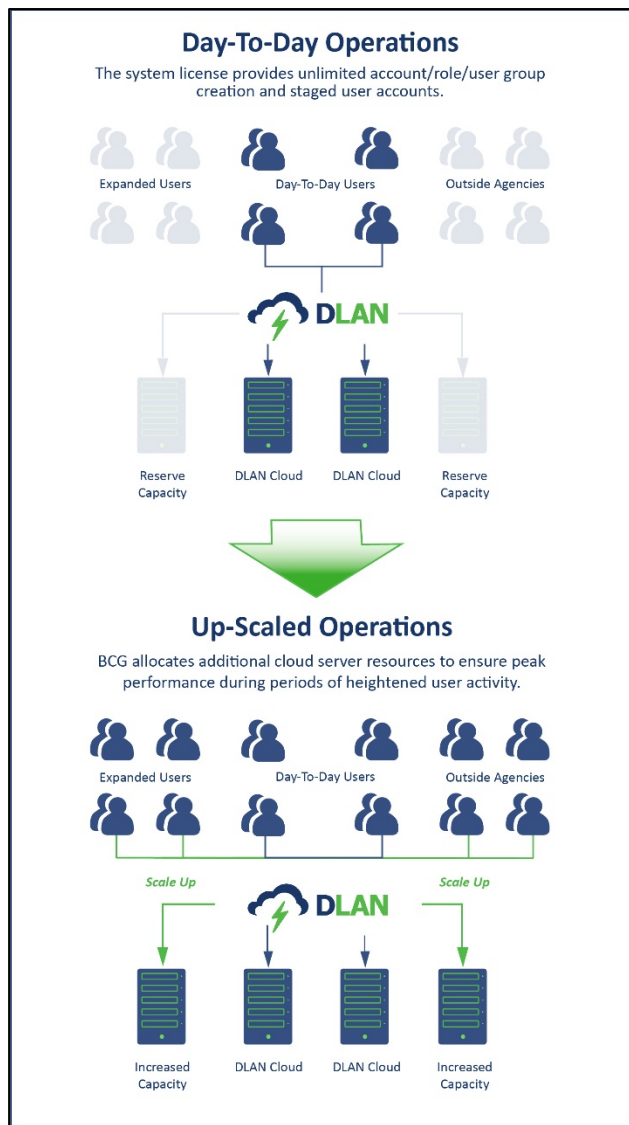


Figure 23: Scalability

4.2.1.3.11 *The EMIS shall adhere to industry standard scalable relational database architectures that are able to provide input or output to other Enterprise systems.*

DLAN’s database runs on Microsoft SQL Server version 2012 or later (newer versions preferred). Any standard method of data exchange supported by SQL should be available to use with the DLAN software system.

4.2.1.3.12 *The EMIS’s Graphical User Interface (GUI) shall be a windows-based interface, and mobile app User Interfaces (UI).*

DLAN is a web-based software system that runs on MS SQL and IIS and can be accessed from any computer, laptop, or device that supports a modern web browser (IE 11, Edge, Chrome, Firefox, or Safari) as well as browsers on mobile device such as chrome, android, and safari for iOS. DLAN is useable on both Windows and Mac systems. The DLAN Mobile Responder App is available for iOS, Android, and as a Windows App.

4.2.1.3.13 The EMIS shall have three environments: production, training, and development environments. The training and development platform shall have the same functionality and capabilities of the production platform. The development platform will be used for change management. The training platform will be used for training, exercises, and scenario modeling.

BCG will provide a development, training, and production environment. These platforms are separate so that the data will stay separated. The same features and functionality are available on all environments.

4.2.1.3.14 The EMIS shall have complete redundancy across all components and a sole Disaster Recovery solution, in the event of data corruption, hardware malfunction, or cyber- attacks.

DLAN supports multi-node configurations, virtualization, high availability, load balancing, and disaster recovery. DLAN is also a secure solution and follows guidelines for NIST 800-53 and NEIM. DLAN receives regular security and penetration testing by multiple customers per year. All tests are run by reputable third parties and BCG works with customers to address any potential threats.

For this solution BCG will provide a sole Disaster Recovery solution that will safeguard data and allow the system to be returned to operation in case of impact the primary and secondary replication sites.

4.2.1.3.15 The EMIS shall have multi-server fault-tolerant architecture with full redundancy and automatic recovery.

DLAN uses a multi-server fault-tolerant architecture. It can support redundancy through active/active or active/passive servers for load balancing, failover, and recovery.

BCG asked several clarification questions during the Q&A period as well as asking for clarification on the answers provided by VWDEM after addendum #2 was issued. BCG is providing the following attributes based on our best understanding of the desired system architecture as described in the RFP and Addendums. However this approach can be adjusted prior to contract award if needed. Please see Figure 24: Cloud Hosting Specifications below.



Figure 24: Cloud Hosting Specifications

- BCG will provide adequate burstable bandwidth to support system performance for VWDEM.
- BCG will use VPN over the public internet for transfer, or simple TLS 1.2 encryption for transport.
- BCG will provide adequate file share storage (up to 1 Terabyte).
- BCG assumes 99.9% guaranteed uptime for system availability not including planned updates. Realized annual uptime on BCG systems is often closer to 99.99%.
- Disaster recovery or failover between sites may require some brief manual intervention by BCG’s 24x7x365 support engineers. Disaster recovery or failover may incur additional costs or services that are not covered in the basic monthly charges and will be provided at a time and materials basis by BCG pending WVDEM’s approval.

4.2.1.3.16 *The EMIS shall support multi-site architecture that provides for the following replication sites and supports an Active/Active platform for high- availability and load balancing. The sites must meet the following minimums.*

1. *Primary replication site at least 50 miles from our facility.*

BCG shall provide an Active/Active platform for hosting of the EMIS application using Amazon Web Services with availability zones for redundancy and high availability. BCG shall provide load balancers to direct traffic

to the appropriate server. The hosting shall support up to 500 concurrent users with the capacity to surge user connections in excess of that number if needed.

BCG will provide the Primary replication site in AWS' Virginia location which will meet the requirement for it to be at least 50 miles from WVDEM's facility.

2. Secondary replication site at least 100 miles from our facility and at least 100 miles from the primary replication.

BCG will provide a secondary replication site located on in Ohio, which will meet the requirement that the site be at least 100 miles from WVDEM's facility and the Primary site.

3. Tertiary replication site at least 200 miles from our facility. and at least 200 miles from the secondary replication.

BCG will provide a tertiary replication site in California, which will meet the requirement that the site be at least 200 miles from WVDEM's facility and the Primary site.

BCG will provide a target Recovery Time Objective (RTO) of 72 hours and a target Recovery Point Objective (RPO) of 24 hours.

The vendor shall provide a copy of their disaster recovery plan upon Agency request.

BCG agrees to provide a copy of our disaster recovery plan upon Agency request.

4.2.1.3.17 The EMIS shall provide data backup to include error checking and correcting during backup to ensure backed-up data is valid.

DLAN supports backups through any software or platform that supports operation on MS SQL server databases. This includes the ability to error check and correct data during a backup to ensure data is valid. BCG is proposing an on-premise installation for this project so the state would be able to implement a backup solution of their choice. Data replicated to the primary, secondary, and tertiary replication sites can also be backed up.

4.2.1.3.18 The EMIS shall provide for records maintenance and retain information until permanently deleted.

DLAN logs and maintains all records within the system. Typically, deleted data is "soft deleted" meaning that it is hidden from display to the user, not removed from the database. Typically, there is no reason to permanently delete record data within DLAN as data can be archived or soft deleted when no longer needed.

4.2.1.3.19 The EMIS shall provide flexible emergency management support functions for day-to-day operations and large-scale multi-agency response.

DLAN is specifically designed to support daily operations and emergency responses. Integrating Incident Management Software into daily operations is the gold standard for getting staff familiar with the software and prepared to utilize it during an emergency. BCG highly recommends customers find ways to utilize the software in daily operations and provides several tools that can be used on a daily basis for normal operations, including

event logging, social media monitoring, email monitoring, webpage/RSS feed monitoring, documentation library folders, role-based briefing notes, and several other tracking tools.

In addition to these daily use monitoring and documentation tools DLAN provides a common platform for task, resource, and information management system that can be applied to various types of needs and workflows. Documentation management and sharing is another area that sees regular system usage within daily operations through the use of our Reference Library. DLAN can be used to monitor incoming information and easily move from event monitoring to emergency activation.

DLAN is designed to work across multiple agencies with features such as location and group based access, user and role based boards, multi-tiered security settings, and incident locking. The permissions structure in DLAN can be configured by the customer to have granular security permission, broad security permissions, or any range in between. Using these same security permissions whole incidents can be locked down to only specific facilities. In this way DLAN balances the need for collaboration and the need for privacy among multiple agencies and stakeholders. Additionally, DLAN provides for the development of contact lists and personnel databases to support communication across multiple agencies and the custom development of standard operating procedures and checklists to facilitate a unified response.

4.2.1.3.20 The EMIS emergency management support functions shall enable users to share, analyze, and prioritize information across multiple jurisdictions in text, images, and geo-referenced map formats.

DLAN allows information to be shared across multiple jurisdictions in numerous formats including text, images, and geo-referenced map formats. With DLAN users from different jurisdictions and agencies can work together on a common unified platform to share, analyze, and prioritize information for an improved response effort. Text, images, and maps can be posted to a Status Board (dashboard) to share them with other jurisdictions. This information can also be shared within other modules and system features such as tickets, messages, emails, file storage libraries, and GIS map reports.

4.2.1.3.21 The EMIS shall operate as a web application in which users interact with the EMIS through any web browser, and mobile applications.

DLAN is a web-based solution that is able to work across multiple OS platforms, browsers, and mobile devices. Please see Figure 25: Browser and Device below.

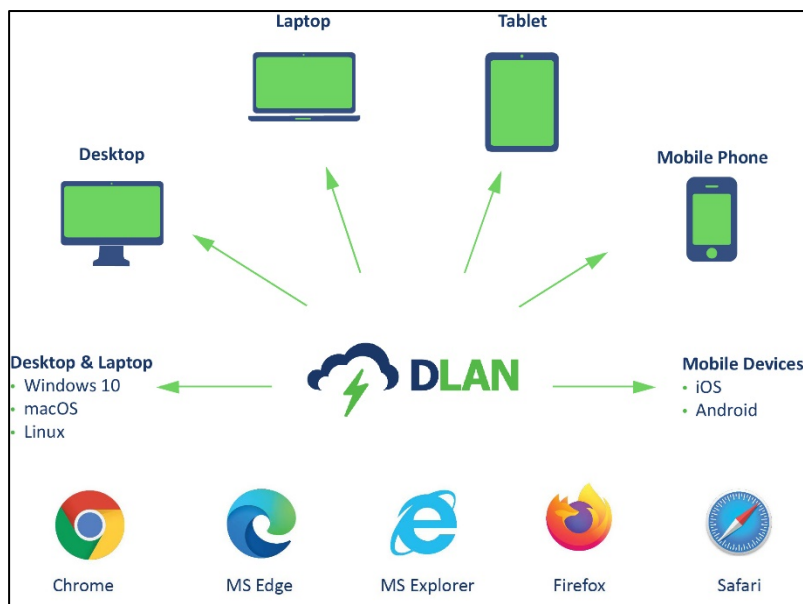


Figure 25: Browser and Device Compatibility

DLAN testers and engineers test DLAN modules and tools on several browsers to ensure that the platform can be used on the greatest number of browsers as possible. This includes testing the product on Internet Explorer 11, Edge, Firefox, Safari, Safari on iOS, Chrome, Chrome on Android, and Android browsers.

In general, DLAN is designed to be accessible from any mobile browser that fully supports JavaScript, session-based cookies, HTML 5 technologies, and other modern web browser features. DLAN’s responsive design interface allows many mobile devices to support DLAN natively (i.e. no app required) including Apple iOS Devices, Windows Mobile Devices, and Android Devices.

Since modern browsers are regularly updated, BCG developers are constantly reviewing and retesting on all major browser platforms so that they can identify changes or issues and adapt the system to work on the widest range of browser platforms as possible. An agile development process and regular product updates (typically every 8-10 weeks) allows DLAN to remain web and mobile browser agnostic.

4.2.1.3.22 *The EMIS shall be browser independent, and device awareness industry requirements.*

The DLAN EMIS is browser independent, supporting the latest versions of Chrome, Edge, Firefox, and Safari on desktop, and Chrome and Safari on mobile devices. DLAN is accessible from any modern mobile devices through the device’s web browser. Additionally, a native mobile application is available for iOS and Android devices.

4.2.1.3.23 *The EMIS shall be built on a highly secure platform. The Vendor shall describe their platform and security measures such as end-to-end encryption.*

DLAN is fully compliant with the AES256 standard. Passwords and other sensitive information are encrypted in the database using AES with 256 bit keys. In addition, all encrypted data is indexed with a hashed lookup code so it is impossible to determine what the data context is without previous knowledge of the key used to store the information. During transmission DLAN relies on HTTPS using TLS for client to server communications. For Internet mail capabilities transmission can occur in plain text, SSL, or TLS.

DLAN passes a biannual security audit conducted by a State Level Department of Homeland Security and Emergency Services who utilize DLAN for their operations. This scan looks for vulnerabilities in IIS, .Net, SQL, and other components of all forward facing websites deployed. DLAN has also passed independent security audits for multiple customers on all system components. Third party system reviews were conducted by established and reputable audit firms such as C2 and Deloitte. BCG is also a member of the Federal Bureau of Investigation’s Infragard team dedicated to identifying and neutralizing threats to critical infrastructure and software and has a full-time CISSP employed on staff.

4.2.1.3.24 *The EMIS shall provide secure usage capabilities such as security reporting, user data access, and email/message.*

The DLAN EMIS is a secure system. The System Administration pages provide authorized users and administrators access to standard reports, user information, message queue data, and monitoring capabilities:

Admin: Site Security	
Users	Groups
Roles	Modules
Reports	
Report Name	
Currently Locked Out Users	
Currently Logged in Users	
Group Modules	
Mobile Responder Users	
Module Users	
Routing Permissions - Who a Role Can Route to	
Routing Permissions - Who Can Route to a Role	
Security Violations	
User Activity	
User Agreement Compliance	
User Groups / Incidents	
User Groups / Modules	
User Groups / Modules / Items	
User Login History	
User Login Timeline	
Users Last Changed PWs	
Watch Command Activity	

Figure 26: Administrator and Usage Reports

In addition to the standard reports shown in Figure 26: Administrator and Usage Reports, the system also provides a message queue page that lists all email/messaging records, their status, and other key information.

4.2.1.3.25 *The EMIS shall enforce secure networking protocols and ports for all activities.*

DLAN adheres to and utilizes multiple ratified and draft RFC standards in its implementation. These include, but are not limited to:

- SMTP (5321, 6152)
- MIME (2045, 2046)
- POP3 (1939)
- IMAP (3501)
- TCP (793)
- IP (791)
- UDP (768)
- RPC (5531)
- TIFF (3302)
- HTTP (2616, 2617)

4.2.1.3.26 The EMIS shall maintain an event log of all entries, which makes a time-stamped record of receipt and transmission of messages.

All information added or modified in DLAN is automatically date and time stamped and displayed in the user interface. All messages and entries are logged along with a record of receipt and pertinent information. Event logs are available both during and after an incident, and historically can be accessed by administrators for view at any time. They are helpful for creating after action reports.

Additionally, history tracking reports are available from a number of different modules in DLAN. The event log history is available for all log entries and shows who created, viewed, or edited the item. An event history by user is available using the Role Activity Log report. When an event or incident is completed it can be deactivated/archived. Archiving an incident makes it unavailable to general users, but administrators or designated users can access it for reporting and analysis or reactivate it as needed. All previous incident responses and their event/ticket log history are archived in the system for easy after action reporting or for auditing purposes.

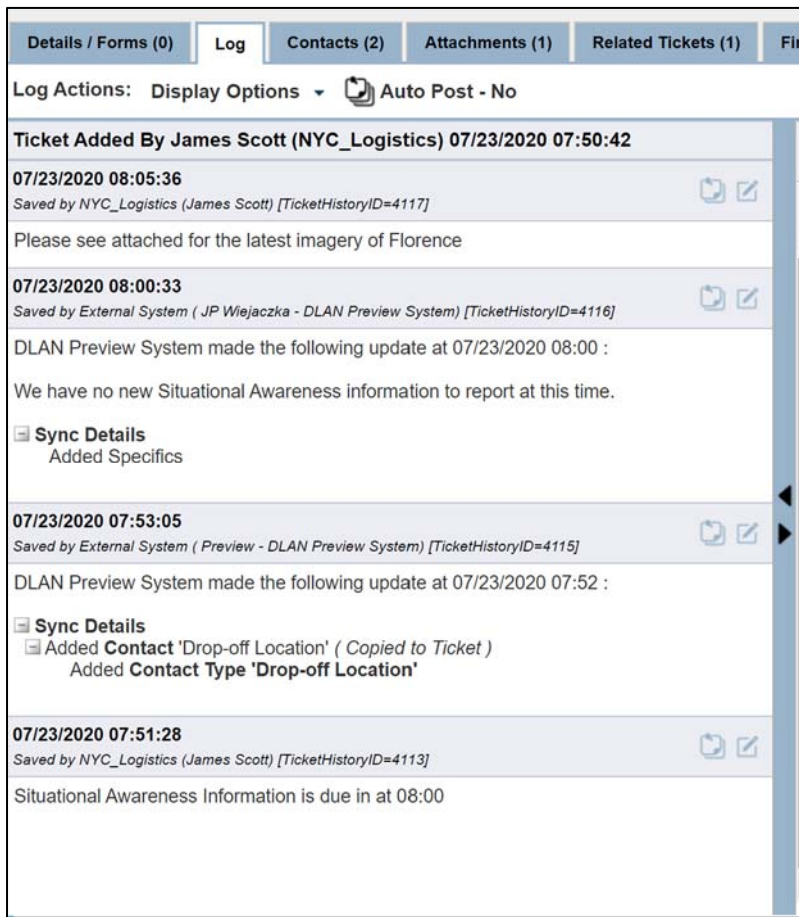


Figure 27: Event Log

Another example is the Status Board History Tracking Report. The Status Board Module tracks all changes made to each board. From the print board screen history tracking can be turned on and a date range can be selected to produce a history tracking report.

4.2.1.3.27 *The EMIS shall create and maintain a security audit trail to log system usage.*

DLAN is a fully audit ready system with full incident reporting and history tracking to support audit trail capabilities. The Incident Report feature provides a full chronological log of all system usage. The report can be run at the end of an incident before it is archived, or it can be run as a spot report at any point while the incident is active.

All information within the system is logged and time-stamped as illustrated by the Incident Report below.

Incident Report: Summer Storm

Downloads: [Incident Action Plans](#) [ICS Forms](#) [Situation Reports](#) [Incident Folders](#) [COP Screen Shots](#)

Start Date: 11/1/2017 End Date: 12/14/2017

Type: Tickets; DMail Messages; Statu Order Items: Chronologically Run Report

1 of 1 | Export to the selected format | Export

Incident Report as of 12/14/2017 11:08:53 AM For Incident: Summer Storm
Includes Items Of Type: Tickets, DMail Messages, Status Boards, Broadcasts, Situation Reports, Form Instances, IAPs, Folders and Resources, COP Screen Shot
Includes Items from 11/1/2017 12:00:00 AM to 12/14/2017 11:08:53 AM
Ordered: Chronologically

11/8/2017 4:15:07 PM - Incident Action Plan Created On: 6/29/2016 2:17:55 PM. Modified by Cerra, Patrick
12/7/2017 3:16:40 PM - Ticket Manager Ticket - 3224 Created On: 6/2/2016 9:57:40 AM. Modified by Cerra, Patrick (Finance & Administration Section Chief) Ticket Modified as follows: Added the following specifics: Incident Command has approved expenses for additional beds and resources to be provided to the Main St. Shelter. Additional details to follow.
12/13/2017 3:28:37 PM - Ticket Manager Ticket - 3295 Created On: 10/17/2016 9:28:29 AM. Modified by Thompson , Ava (Logistics Section Chief) Ticket Modified as follows: Added the following specifics: Team Assigned.
12/13/2017 3:29:11 PM - Ticket Manager Ticket - 3295 Created On: 10/17/2016 9:28:29 AM. Modified by Thompson , Ava (Logistics Section Chief) Ticket Modified as follows: Changed status to Assigned to Location

Printed on: 12/14/2017 11:08:53 AM 1 of 1

Figure 28: Event Log & Incident Report

4.2.1.3.28 *The EMIS shall have an automated and scheduled back up of information, including back up of image libraries, recording libraries, and document libraries.*

BCG will provide a backup service for the EMIS. Backups include both the database and file storage. Typically, BCG provides 15 minute incremental backups with daily full backups. These can be set to run at a scheduled time such as off-hours in order to reduce any potential impact to performance.

4.2.1.3.29 *The EMIS shall support interaction with remote users using a workstation, laptop, tablet, and mobile devices.*

DLAN is a web-based application that can be used on a workstation, laptop, tablet, or mobile device. For additional compatibility information, please refer to Figure 25: Browser and Device Compatibility.

4.2.1.3.30 *The EMIS shall be able to access, integrate, interoperate, and remain compatible with the Agency GIS platform (ESRI - ArcGIS).*

BCG has been providing ESRI based GIS Mapping capabilities inside the DLAN EMIS since 2004. The system is integrated with the Agency’s ESRI ArcGIS platform out of the box. All basemaps, geocoders, layers, and services are compatible. ESRI ArcGIS dashboards and experiences are also compatible and can be displayed in a DLAN Status Board. Additionally, DLAN’s integration with ArcGIS functions with both Enterprise/Portal and ArcGIS Online. Data can be synced in real time between the DLAN ticket manager module, assets module, and other system data sets and ArcGIS.

4.2.1.3.31 *The EMIS shall have an alternate GIS platform that can be used if the Agency GIS platform source is unavailable.*

DLAN is fully integrated with ESRI’s ArcGIS Online. Ticket Report data can be synced in real time to ArcGIS Online (AGO) for either public or private viewing and (if permitted) editing on the AGO platform. DLAN’s integration with AGO also supports the ability for users to fill out forms on the AGO map and sync the data back to DLAN. The system also supports Open Geospatial elements and GeoJSON data services if needed.

4.2.1.3.32 *Support and Maintenance of the EMIS for the period of the contract shall include all upgrades or enhancements, bug fixes, document changes, system support including a technical hotline and support services to support the requirements of this system.*

For this project BCG is proposing our **Gold Plus Support package**, which includes everything West Virginia requires. It will provide all upgrades and enhancements, bug fixes, online document changes, system support including a technical hotline and support services to support your staff and the requirements of your system. The Gold Plus Support Package we recommend is defined as follows:

Maintenance & Support Service Provided *	Gold	Plus
Business Day (9am – 5pm PST) Email and Phone Support	✓	Plus can be added to any support package
24/7 Emergency Activation Phone Support	4 cases per year	
BCG Assisted Patching Support	24/7	
New Releases of Product	✓	
New Release Review Webinars	✓	
Hot Fixes for New Releases	✓	
Point Patches for New Releases	✓	
Rush Delivery of Hot Fixes Specific to Organization’s Site or Installation		
Server Node Support	Up to 2 Nodes	
Custom BCG Services	40 hours per year	

Onsite Support		
Unlimited 24/7 Support		✓

*Terms and Conditions Apply

4.2.1.3.33 The Vendor shall provide a proposed EMIS support model. The proposed support model must identify how the vendor will address the ongoing support functions.

BCG believes that the high level of support we provide to our customers sets us apart from our competition. We constantly elicit customer feedback and incorporate it into making DLAN a better product. Customer input is always important in the decisions that are made to provide new feature enhancements. If the BCG team feels that a requested customization will be beneficial to other customers, it may be developed at a significantly reduced cost or at no cost and then provided to all customers with a current maintenance & support package.

Help Desk (24x7x365 for WVDEM)

All reported issues will be addressed by the BCG Client Services team. Customer service is a key component to any solution. BCG understands some customers prefer self-service features over working with customer service. BCG also understands a solid help desk is essential to providing top tier support. BCG’s best in class support model and software utilize both methods to provide ease-of-mind as well as ease-of-use.

The BCG Software System includes an online help section that allows users to reference help articles for all pages in the system. Users will also have access to the training materials and quick reference guide developed by the BCG Team for this project.

In addition to this self-service help, the BCG Team will provide a business day customer support help desk that is available to the State. The help desk includes a ticketing system, phone, and email support as needed. BCG also provides an escalation process that helps us respond quickly to customer issues (see Figure 29: Support and Escalation).

BCG provides direct access to product engineers if requested by a customer through the help desk. This streamlines the support process, eliminating the need to progress through multiple tiers of support to obtain problem resolution. All BCG Team engineers are equipped with the skill set required to adequately troubleshoot, and diagnose issues. It is the BCG Team’s assumption that help requests that are submitted by users would be collected and vetted by the State’s system administrators before escalation to the BCG Support Team. All BCG support team staff are full time employees of BCG based out of our USA offices.

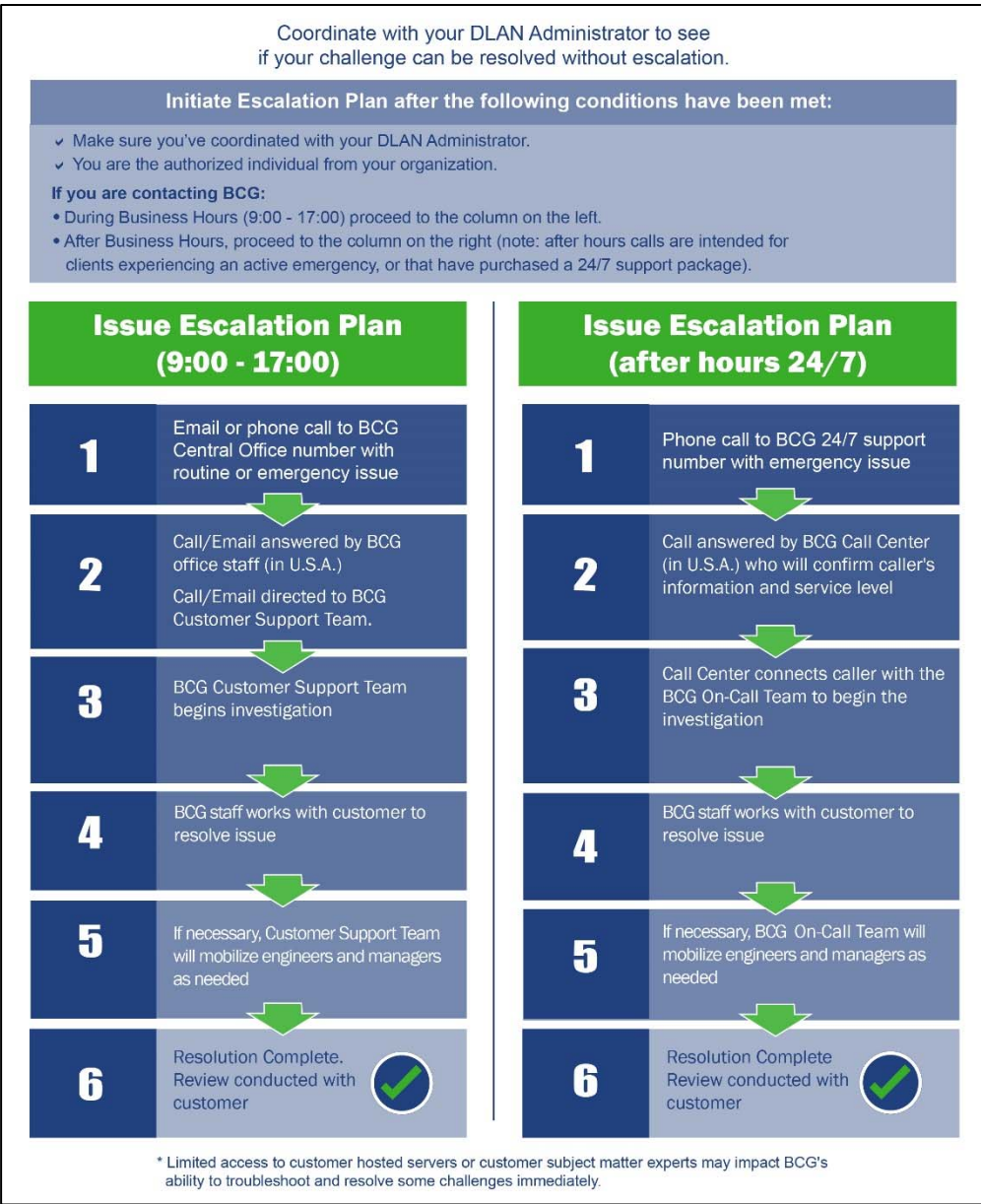


Figure 29: Support and Escalation

4.2.1.3.34 *The Vendor shall provide a proposed EMIS maintenance schedule and services schedule with costs and any additional service packages.*

BCG provides a required maintenance and support package for each DLAN system that entitles the customer to receive all updates to the software, including new versions, at no extra licensing cost. All DLAN versions are forward and backwards compatible by design and legacy data is always protected and supported. BCG uses an agile development methodology for DLAN and typically has updates available every 8-10 weeks. The state can choose how often they want to accept these DLAN updates, but BCG recommends at least bi-annually or annually. For security and support reasons, typically BCG does not support legacy versions of the software under standard maintenance for more than two years from date of issue unless specifically stipulated in a contract.

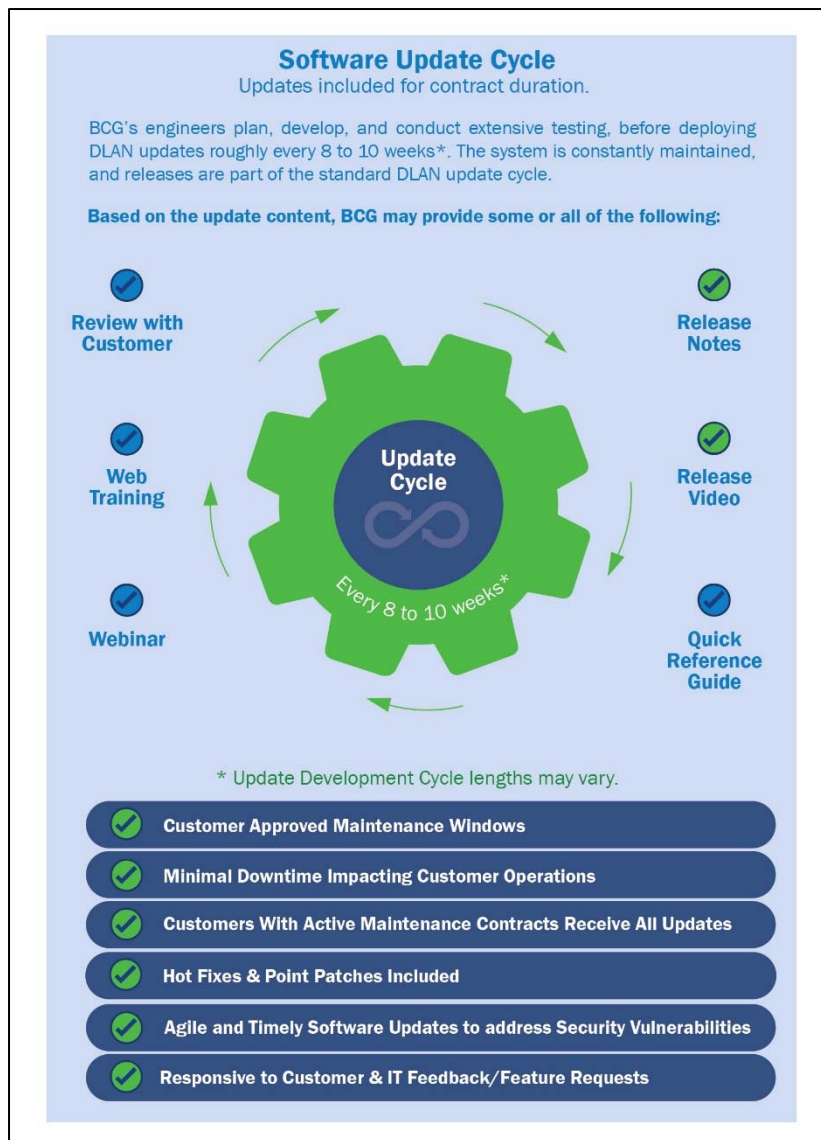


Figure 30: Continuing Support Cycle

4.2.1.3.35 *The EMIS shall provide a cyber-secure environment and a continuity plan in case of a system failure*

DLAN provides a cyber-secure environment and a continuity plan for all hosted systems. DLAN supports multi-node configurations, virtualization, high availability, load balancing, and disaster recovery. DLAN is also a secure solution and follows guidelines for NIST 800-53 and NEIM. BCG is also ISO 27001 certified. DLAN receives regular security and penetration testing by multiple customers per year. All tests are run by reputable third parties and BCG works with customers to address any potential threats in an expedited manner.

4.2.1.3.36 *The Vendor shall provide 24/7 technical support to sustain continuous operation. Vendor must provide support by telephone, online, and email 24 hours a day, 7 days a week, 365 days a year for troubleshooting technical issues.*

BCG is providing our 24/7 Gold Plus Level Support as described above (**Gold Plus Support**), including 24x7x365 access to BCG technical support team members through email, web, and telephone.

The Vendor will provide the following response times to request for technical support:

- 1. No more than one (1) business day for non-critical issues.*

BCG agrees to respond to requests for non-critical issues within (1) business day.

- 2. No more than two (2) hours for critical issues.*

BCG agrees to respond to requests for critical issues within (2) hours.

BCG's response service levels typically exceed what is asked for here. For additional service level information, please refer to BCG's service level chart, which is located in the Master Services Agreement on page 115.

4.2.1.3.37 The EMIS will be hosted on a minimum of a Tier 3 Data Center and have cloud-based hosting. Upon Agency request, the vendor shall provide a minimum of a Tier 3 data center certification verifying that it meets the following standards:

- 1. ISO 27001*

BCG has successfully completed the process of certification for ISO 27001, along with our HIPAA certification. In addition, BCG's engineers and quality assurance teams check all code against industry best practices including OWASP and SANS' top twenty list. BCG also maintains a disaster recovery and business continuity plan based on NIST 800-34r1. BCG's standard cloud datacenters perform SSAE 16 SOC2 Type II audits annually. They have achieved ISO 9001:2008, 27001:2013 and PCI 3.0 certification.

- 2. NIST SP800-53.*

BCG's business practices and the DLAN Product are in line with the controls listed in NIST SP 800-53. BCG works annually with third party security consultants to review our NIST SP800-53 controls and ensure we remain compliant and all practices are in line with the standard. This is in addition to our ISO 27001 certification.

4.2.1.3.38 The EMIS must be capable of being hosted on a minimum of a Tier 3 Data Center with a combination of local servers at the agency and have cloud-based hosting.

BCG uses Tier 3 or better Data Centers for all cloud hosting services. For this project, BCG proposes an Amazon Web Services (AWS) based cloud hosting solution managed by BCG and long-time datacenter partner Lumen.

Lumen

Lumen offers high-availability application hosting. Lumen offers a number of service options which include high SLAs, failover and redundancy. Servers will be in a secured facility (24/7/365). These facilities have enhanced security measures such as key card access, a secondary biometric authentication and video surveillance. Each data center holds several certifications and compliances (e.g. PCI DSS, SOC 2 TYPE II). A list of security features, certifications and compliances for a particular data center can be provided upon request.

Other Cloud Platforms

If Amazon Web Services cloud hosting is not desirable, BCG will work with your IT team to find a hosting platform that will meet your specific needs. In addition to our main hosting partners, BCG can also provide hosting through Microsoft Azure, Lumen, and other providers.

Additional Services

In addition to our base hosting packages, DLAN can provide a number of additional services including higher SLAs, disaster recovery, dedicated hardware, and additional surge capacity. BCG can work with your IT team to find a hosting environment that will meet your specific needs.

4.2.1.3.39 Vendors must provide a detailed response for each section in the specifications on how they meet or exceed the mandatory requirements. Vendors who fail to provide the required specification sheets within the allotted timeframe will be disqualified. This will require EACH SPECIFICATION to be detailed in bid submission. This shall be submitted as a WORD document or EXCEL document.

BCG has provided a detailed and thorough response to each section and requirement in the specifications list.

4.2.2 Contract Item 1: Annual Subscription for EMIS Solution

4.2.2.1 Vendor must provide an annual cloud-based subscription for EMIS Solution as defined in Section 4.1.1.

BCG shall provide an annual cloud-based subscription for the DLAN EMIS solution it is proposing.

4.2.2.2 Vendor must provide access for an estimated quantity of 500 users simultaneously with the ability to add more users without delay as per Section 4.1.1.3.10.

BCG shall provide access to the system for an estimated 500 concurrent users (accessing the EMIS simultaneously). The system also provides scalability, allowing WVDEM to add more users without delay or need to contact BCG for an increase in user accounts. If WV needs additional cloud resources for a sustained surge in the number of concurrent users they can contact BCG Support and make the request.

4.2.2.3 Vendor must provide the following with the annual subscription:

4.2.2.3.1 Maintenance and support services.

BCG will provide for ongoing update and maintenance of the system. This will include any bug fixes and updates that take place during the contractual period. BCG will coordinate any software updates and hardware maintenance with WVDEM to minimize impact to daily ongoing operations. If WVDEM is experiencing an emergency, they can request that BCG hold any updates until concluded.


4.2.2.3.2 Module customization, and setup.

BCG will configure the DLAN system to match WVDEM's desired status boards, forms, workflows, and settings to meet the State's needs. BCG will configure the software to match the desired State EOC organizational structure and operations. BCG will also work with WVDEM to identify key workflows, reporting requirements, communication chains, and system outputs and then configure the system in a way to meet these needs. BCG will

work with WVDEM IT to configure accounts, roles, and security rights for administrative personnel end users. System configuration is a process that occurs over several weeks with knowledge transfer and demonstrations between BCG and WVDEM. BCG will complete most configuration remotely. BCG will also review configuration settings with WVDEM and ask for sign-off of the final system configuration.

4.2.2.3.3 Onboarding for all users.

BCG shall provide onboarding services for WVDEM. A typical example of the onboarding process is below.

Example Standard Implementation Process	
BCG Responsibilities	Customer Responsibilities
 <p>Pre-Planning</p> <ul style="list-style-type: none"> ✓ BCG reviews pre-planning requirements with the customer, and secures all contacts needed. 	<p>Pre-Planning</p> <ul style="list-style-type: none"> ✓ Complete needs analysis ✓ Provide paper process and forms needed ✓ Identify challenges ✓ Outline technologies and integrations ✓ Identify user roles and responsibilities
<p>1</p> <p>Phase 1 - Planning</p> <ul style="list-style-type: none"> ✓ Host kick-off meeting ✓ Establish Project plan ✓ Design workflows 	 <p>Establish Steering Committee</p> <ul style="list-style-type: none"> ✓ Define project guidance and sponsorship ✓ Buy-in and sign-off ✓ Conduct executive review ✓ Identify security groups
<p>2</p> <p>Phase 2 - Configuration</p> <ul style="list-style-type: none"> ✓ Install and test application ✓ Configure dashboards and system ✓ Implement integrations ✓ Provide BCG's specialized knowledge transfer to working group (i.e. IT, GIS) 	 <p>Engage Working Group</p> <ul style="list-style-type: none"> ✓ Inform knowledge transfer and configuration ✓ Compose a working group of key staff (i.e. SMEs, managers, section chiefs, key stakeholder partners, and departments) ✓ Define the working process (day-to-day operations and emergency response) ✓ Identify views for exec, operations, and field
<p>3</p> <p>Phase 3 - Training</p> <ul style="list-style-type: none"> ✓ Distribute training plan and materials ✓ Conduct UAT, security scans, performance test (if needed) before training ✓ Complete user and admin training • Conduct exercise scenario (optional add-on) • Provide after action review (optional add-on) 	 <p>Working Group</p> <ul style="list-style-type: none"> ✓ Conduct UAT, security scans, performance test (if needed) before training ✓ Identify training levels and attendees ✓ Determine if training is on-site, remote, or hybrid ✓ Approve training deliverables
<p>4</p> <p>Phase 4 - Deploy System</p> <ul style="list-style-type: none"> ✓ Sign-off and go live ✓ Continuous support 	 <p>Working Group Becomes User Group</p> <ul style="list-style-type: none"> ✓ Sign-off and go live ✓ Continuous operations

Each customer implementation has unique parameters. Changes to the implementation process or requirements may affect the above example.

Figure 31: Implementation Process Example

In addition to onboarding, BCG has allocated for up to 8 days of onsite instructor-led training by BCG trainers. BCG can provide flexible topics and training plans tailored to fit WVDEM's organization. BCG will provide the following training materials: Quick Reference Guides for system administrators, basic users, and advanced users. BCG will also provide a training agenda document to assist WVDEM in scheduling their training activities, Micro-training videos designed for just in time training, and recording of all onsite instructor led training classes to assist with future staff onboarding.

4.2.2.3.4 Continuous access to training for all users.

BCG can provide continuing access to training for all users through both an annual instructor led refresher training and self-help services. For individuals looking to educate themselves at their own pace, BCG offers a built-in Online Help system with 375 user focused articles covering all topics in the system. Additionally Quick Reference Guide training materials and links to training videos will be loaded into the system for users to review.

4.2.2.4 Vendor must sign and return the attached Software as a Service Addendum prior to award of the contract.

This document is signed and attached in section [11.2 Software as a Service Addendum](#) below on page 88.

4.2.3 Acceptance of System

4.2.3.1 If the test period produces no issues at a minimum, the Agency will issue a Letter of Acceptance of the system, and the contract and annual license would start at that time.

BCG agrees to an acceptance period for the system. The contract and annual license will not start until the system has been accepted.

11. MISCELLANEOUS

11.1 Contract Manager

Contract Manager:	Gary F. Masterson
Telephone Number:	(716) 822-8668
Fax Number:	(716) 822-2730
Email Address:	gmasterson@bcgeng.com

11.2 Software as a Service Addendum

See attached

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
 - 10 days after the effective date of termination, if the termination is in accordance with the contract period
 - 30 days after the effective date of termination, if the termination is for convenience
 - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: WV Emergency Management Division

Signature: _____

Title: _____

Date: _____

Name of Vendor: Buffalo Computer Graphics, Inc

Signature: Ray J. Musterson

Title: PRESIDENT

Date: 3-Dec-2021

APPENDIX A

Version 11-1--19

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: BUFFALO COMPUTER GRAPHICS, Inc.

Name of Agency: West Virginia Emergency Management Division

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes
No
2. If yes to #1, does the restricted information include personal data?
Yes
No
3. If yes to #1, does the restricted information include non-public data?
Yes
No
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes
No

5. Provide name and email address for the Department privacy officer:

Name: PATRICK LUPIANI

Email address: PLupiani@bcgeng.com

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: PATRICK LUPIANI

Email address: PLupiani@bcgeng.com

Phone Number: 716 822 8668

EXHIBIT A – PRICING

**EXHIBIT A – Pricing Page
Emergency Management Information System
CRFQ 0606 HSE2200000005**

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Initial Year	Annual	1	\$263,021.01	\$263,021.01
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 2	Annual	1	\$126,828.59	\$126,828.59
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 3	Annual	1	\$126,828.59	\$126,828.59
4.1.2	Contract Item #1: Annual Subscription for EMIS Solution - Optional Year 4	Annual	1	\$126,828.59	\$126,828.59
Overall Total Cost				\$643,506.78	-

Please note: This information is being captured for auditing purposes.
 Any product or service not on the Agency provided Cost Sheet will not be allowable. The state cannot accept alternate pricing pages, failure to use Exhibit A Cost Sheet could lead to disqualification of vendors bid.
 Quantities listed herein are for bid evaluation purposes; no guarantee of any actual order quantities should be implied.
 Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

BIDDER /VENDOR INFORMATION:

Vendor Name:	BUFFALO COMPUTER GRAPHICS, Inc.
Address:	4185 BAYVIEW RD.
City, St. Zip:	BLASDELL, NEW YORK 14219
Phone No.:	716-822-8668
Email Address:	RFPTEAM@BCGENG.COM

Gary D. Masterson

Vendor Signature:

21-Dec-2021

Date:



SIGNED PURCHASING AFFIDAVIT

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Buffalo Computer Graphics, Inc

Authorized Signature: Ray J. Masterson Date: 3-Dec-2021

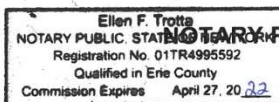
State of New York

County of Essex, to-wit:

Taken, subscribed, and sworn to before me this 3rd day of December, 2021.

My Commission expires April 27, 2022.

AFFIX SEAL HERE



Ellen F. Trotta

Purchasing Affidavit (Revised 01/19/2018)

SAMPLE BCG MASTER SERVICES AGREEMENT

BCG MASTER SERVICES AGREEMENT (MSA)

Updated 12/21/2021

This is a Master Services Agreement effective as of the Effective Date (as defined below) between: _____, a company having its principal place of business at _____ (the "Client") - AND -

Buffalo Computer Graphics, Inc., a company incorporated pursuant to the laws of the State of New York having its principal place of business at 4185 Bayview Road, Blasdell, New York 14219 ("BCG" or "Buffalo Computer Graphics").

For valuable consideration, the receipt and sufficiency of which is acknowledged, Client and Buffalo Computer Graphics (collectively, the "Parties" and each a "Party") agree as follows:

Composition of Agreement

This Master Services Agreement (including all exhibits attached hereto) ("**MSA**") is effective as of the date that the last Party executes this MSA (the date as indicated on the execution page of this MSA) (the "**Effective Date**"). The "**Agreement**" includes this MSA, the SLA, any Order Form(s) and/or Statement(s) of Work ("**SOW**"), the Acceptable Use Policy, which together constitute the entire agreement between the Parties with respect to the subject matter hereof and supersedes all proposals and prior discussions and writings between the Parties with respect thereto.

In the event of a conflict between the terms and conditions of the terms and conditions of any document comprising a part of the Agreement, the order of precedence shall be as follows:

- a) Exhibit A ("Acceptable Use Policy");
- b) this MSA;
- c) Exhibit E ("MSA/SLA Amendments");
- d) Exhibit D ("BCG Service Level Agreement");
- e) The applicable Terms and Conditions;
- f) The Order Form and/or SOW, unless either Order Form and/or SOW specifically states that a provision is to take precedence over a particular document; and
- g) All other exhibits.

1. Definitions

"**Acceptable Use Policy**" or "**AUP**" means the principles, rules and regulations that govern the use of the Services by Client as stated in the Buffalo Computer Graphics Policies attached hereto as Exhibit "A";

"**Bandwidth**" means the range of data transfer speeds measured in bits per second that a network can use. The greater the Bandwidth, the more information can be transferred over that network at one time.

"**Billing Commencement Date**" means (as applicable) the date specified on the Order Form or SOW or, if not specified, the date on which:

- a) Client is notified that Buffalo Computer Graphics is ready to accept the Client Hardware in the case of a Colocation Service;
- b) the operating system has been installed and the Managed Service is ready to accept Client's data in the case of a Managed Service; or
- c) two (2) months after the Effective Date if (a) through (b) above have not yet transpired.

"**Carrier**" means the company contracted by Buffalo Computer Graphics to supply telecommunications facility to the Client location on behalf of Buffalo Computer Graphics.

“Confidential Information” means all trades secrets and other proprietary information owned or licensed by one of the Parties or by any company affiliated with one of the Parties. Confidential Information includes, without limitation, licensed software, all feature sheets, pricing information, inventions, processes, algorithms, source code, client lists, financial information, legal, compliance, corporate, marketing, personnel, product, research, and other non-public information, in whatever form or media. Notwithstanding the foregoing, “Confidential Information” shall not include information which:

- (a) is or becomes generally available to the public other than as a result of its disclosure by the receiving Party or its representatives in breach of this Agreement or which the receiving Party knows (or ought reasonably to have known having made reasonable enquiry) to have been in breach of any other undertaking of confidentiality addressed to the disclosing Party (except that any compilation of otherwise public information in a form not publicly known shall nevertheless be treated as Confidential Information),
- (b) was lawfully in the possession of the receiving Party before the information was disclosed to it by the disclosing Party and continues to be held in accordance with the terms on which it was obtained,
- (c) the receiving Party can establish, through documentary evidence, was developed by or on behalf of the receiving Party without reference to any information disclosed by the disclosing Party, or
- (d) was authorized for release by the disclosing Party in writing.

“Custom Application” is applicable only in the context of a Managed Service and means those computer programs, including documentation relating thereto, all updates and new releases thereof, owned by or licensed to Client by a third party that are not included as part of the Managed Service. Buffalo Computer Graphics is not responsible for support nor licensing such Custom Applications.

“Client Data” means any data, content or information of Client or its end users that is stored, transmitted, or otherwise processed using the Buffalo Computer Graphics Services. BCG’s obligations with respect to such Client Data shall be exclusively governed by the Data Protection and Privacy Policies and are further subject to all Limitation of Liability provisions of this Agreement.

“Client Hardware” means the computer systems, peripherals, terminals, communications equipment and all other related hardware products owned or leased by, or otherwise under the control of Client as stated in the Client Hardware Inventory Form that has been approved by Buffalo Computer Graphics. Furthermore, any changes to this inventory are the responsibility of the Client to provide advanced written notice to Buffalo Computer Graphics on a go forward basis.

“Client Software” means the operating systems and applications, including documentation relating thereto, all updates and new releases thereof, owned by or licensed to Client by a third party that have been specifically approved by Buffalo Computer Graphics for inclusion as part of the Client System but not specifically identified by a Buffalo Computer Graphics Managed Services contract for support by Buffalo Computer Graphics. Furthermore, Buffalo Computer Graphics will not be responsible for licensing nor maintaining this software.

“Client System” means collectively the Client Hardware, Client Software, Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software, all as set out in the Order Form for a Managed Service.

“Facility” means a Buffalo Computer Graphics data center as specified in the Order Form.

“Fees” has the meaning set out in Section 4.1 of this MSA.

“Intellectual Property Rights” means, in respect of any technology, materials, content, or information, all

- (a) worldwide proprietary rights, now or hereafter in force or recognized, provided under
 - i. patent law,
 - ii. copyright law,
 - iii. trademark law (including laws creating rights in Internet domain name registrations),
 - iv. design patent or industrial design law,
 - v. semi-conductor chip or mask work, or
 - vi. any other applicable statutory provision or common law principle, including trade secret law, that may provide a right in such technology, materials, content, or information or the expression or use thereof, and
- (b) applications or registrations, or rights to apply for or obtain registrations, in respect of any of the foregoing.

"Leased Hardware" or **"Buffalo Computer Graphics Hardware"** means any servers, network appliances (e.g., Firewalls, IPS, Storage devices, etc.) utilized by Buffalo Computer Graphics to deliver services to Client.

"Licensed Software" or **"Buffalo Computer Graphics Software"** means any first and/or third-party licenses (e.g., DLAN Software, SQL licenses, Windows OS, etc.) utilized by Buffalo Computer Graphics to deliver services to Client.

"Maintenance Window" means a period of time designated in advance (on a standard recurring or emergency basis) by Buffalo Computer Graphics staff, during which preventive maintenance that could cause disruption of Service may be performed.

"Managed Service" means a data center hosting arrangement where Buffalo Computer Graphics provides all of the components (including both hardware and software) of Client's System to Client and, in addition to providing Facility Services, will install Client's System and will generally configure, back-up, secure and maintain all or a portion of Client's System. On an ongoing basis, Buffalo Computer Graphics ensures the system is up and running in its current state and applies security hot fixes and/or patches for managed applications as considered required by Buffalo Computer Graphics. Application version upgrades and downgrades, unless specifically requested by Buffalo Computer Graphics, are not included in the standard Managed Service arrangement.

"Marks" has the meaning set out in Section 2.13 of this MSA.

"MRC" means monthly recurring charge.

"Network" means the collection of Client locations connected by Buffalo Computer Graphics via one or more Carrier connections so as to enable telecommunications capabilities between such locations and the Facility.

"NRC" means non-recurring charge.

"Order Form" means any Order Form that references this MSA and is executed by both Parties hereto detailing the Buffalo Computer Graphics services requested by Client and agreed to by Buffalo Computer Graphics.

"Services" means the initial and subsequent Buffalo Computer Graphics service(s) provided to the Client as per an Order Form.

"Service Levels" means the predetermined, objective performance criteria for delivery of the Services as stated in the Buffalo Computer Graphics policies.

"Service Level Agreement" or "SLA" means, with respect to a specific Service, a level of performance at which Buffalo Computer Graphics is contractually obligated to deliver the Service to Client and which, depending on the specific Service ordered, is established with reference to certain metrics. If applicable, such metrics are outlined in the attached Service Level Agreement.

"Statement of Work" or "SOW" means the document which defines project-specific activities and deliverables for the Service(s) specified on the Order Form.

"Term" means the duration of time for which the Service is contractually committed. Such duration is indicated in the Order Form or SOW and starts on the Billing Commencement Date.

Any other capitalized term not defined in this MSA shall have the meanings set out in the Terms and Conditions or Schedules, as applicable.

2. General

2.1 Headings. Section headings are provided for convenience of reference only and do not constitute part of the Agreement. Any references to a particular section of this Agreement shall be deemed to include reference to any and all subsections thereof.

2.2 Severability and No Waiver. If any provision of the Agreement is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force without being impaired or invalidated in any way. The Parties agree to replace any invalid provision with a valid provision that most closely approximates the spirit and intent of the invalid provision. The waiver by either Party of a breach of any provision of the Agreement will not operate or be interpreted as a waiver of any other or subsequent breach.

2.3 Assignment. Client may not assign nor delegate any or all of its rights or its duties or obligations under this Agreement without the prior written consent of Buffalo Computer Graphics; provided, however, that Client may, without the prior written consent of Buffalo Computer Graphics, assign this Agreement to an affiliate of Client or to a successor of all or substantially all of the assets of Client through merger, reorganization, consolidation or acquisition. Notwithstanding the foregoing, BCG may increase the Fees if BCG determines, in its sole, reasonable discretion, that an assignment materially increases BCG's cost of providing the services.

2.4 Independent Contractors. The Parties to the Agreement are independent contractors, and no agency, partnership, joint venture or employment relationship is intended or created hereby. Neither Party shall have the power to obligate or bind the other Party. Personnel supplied by Buffalo Computer Graphics shall work exclusively for Buffalo Computer Graphics and shall not for any purpose be considered employees or agents of Client.

2.5 Subcontractors. Buffalo Computer Graphics shall be fully responsible for the performance of all of its obligations under this Agreement, including any obligations performed by a subcontractor.

2.6 Notices. All notices, requests, demands or communications required or permitted hereunder shall be in writing, and delivered by one or more of the following methods (with recognized receipt date):

- a) personally (when delivered)
- b) electronic transmission / email (when acknowledged as received by recipient; note: automatic response does not constitute acknowledgement)
- c) certified or registered mail to the respective addresses as set forth below or at such other addresses as shall be given in writing by either Party to the other (when received and signed for).

2.7 Governing Law, Jurisdiction and Venue. The Agreement created hereunder shall be deemed to have been made in, and shall be construed pursuant to, the laws of the State of New York and any action or proceeding arising out of or related to this Agreement shall be brought only in the federal or state courts located in the State of New York. The Parties hereby irrevocably consent to such jurisdiction and venue.

2.8 Counterparts. The Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

2.9 Force Majeure. "Force Majeure" means an event, the cause of which is beyond the reasonable control of the Party affected thereby and which could not reasonably have been foreseen and provided against, including, without limitation, acts of god, strikes, lock outs or other labor or industrial disturbances, accidents, fires, explosions, interruptions in telephone, electrical, cable, fiber or other services necessary to perform the Services, weather conditions materially preventing or impairing work, inability to secure fuel, power, materials, contractors or labor, mechanical breakdown, failure of equipment or machinery, delays in transportation, wars, civil commotion, riot, sabotage, applicable legislation and regulations thereunder, interruption by government or court orders and future orders of any regulatory body of competent jurisdiction. Notwithstanding any other provision of the Agreement, if by reason of Force Majeure, either Party is wholly or partly unable to perform certain elements of its obligations hereunder, it shall be relieved of those obligations to the extent, and for the period, that it is affected by Force Majeure, provided that the affected Party gives the other Party prompt notice of such inability. The Party affected by Force Majeure shall use all reasonable efforts to remedy the situation and remove, so far as possible and with reasonable speed, the cause of its inability to perform, provided that there shall be no obligation on a Party so affected to settle labor disputes or to test or to refrain from testing the validity of any order, regulation or law in any court having jurisdiction.

2.10 Non-Solicitation. Both Buffalo Computer Graphics and Client agree that during the Term of this Agreement and for a period of one (1) year following the expiration or termination hereof, neither Party shall, directly or indirectly, hire or offer to hire or entice away or in any other manner persuade or attempt to persuade any officer, employee, agent, or client of the other Party to discontinue his or her or its relationship with the other Party. A general advertisement or notice of a job listing or opening or other similar general publication of a job search or availability to fill employment positions, including on the internet, shall not be construed as a breach of this Section and the hiring of any such employees or independent contractor who freely responds thereto shall not be a breach of this Section.

2.11 Amendments. No amendment, modification, supplement or other purported alteration of this Agreement shall be binding upon a Party unless in writing signed by them or on their behalf by a duly authorized representative(s).

2.12 Survival. Sections 2.2, 2.7, 2.10, 2.12, 3.5, 4, 5 and 6 shall survive the expiration or termination of this Agreement along with any other provision of this Agreement which expressly states it is to continue in effect after termination or expiration of this Agreement.

2.13 No Lease. The Parties acknowledge and agree that this Agreement is a services agreement and is not intended to and shall not constitute a lease of or tenancy or other interest in the Facility, any real property owned or leased by Buffalo Computer Graphics or in any Buffalo Computer Graphics Hardware or any other personal property of Buffalo Computer Graphics.

3. Delivery and Term

3.1 Delivery of Services. Subject to Client's compliance with the Acceptable Use Policy (AUP), a copy of which is attached as Exhibit "A", and the Credit Application Form, Services are acquired from Buffalo Computer Graphics by using Order Form(s) and/or SOW(s). Each Order Form and/or SOW shall be on Buffalo Computer Graphics' standard form and must be executed by both Buffalo Computer Graphics and Client prior to becoming effective. Upon each Order Form and/or SOW becoming effective, it shall, along with the applicable Terms and Conditions and the Schedules referenced therein, form a part of this Agreement and be governed by the terms and conditions contained herein. For greater certainty, Client agrees to be bound by this MSA and the applicable Terms and Conditions during the provisioning period, which is defined as the period from the Effective Date to the commencement of the Initial Term. In the event that Buffalo Computer Graphics is unable to provision a particular Service due to lack of Service availability, Client will not be responsible for the payment of such Service and Buffalo Computer Graphics will not be responsible to Client for any costs Client may have incurred in preparation for Service implementation. Client will continue to be bound by this Agreement for all provisioned Services.

BCG hereby grants Client a non-exclusive, non-transferable (except in compliance with Section 2.3) right for Client and its affiliates to access and use the Services during the Term. Such use is for Client and its affiliates' internal use.

3.2 Term and Renewal. Services for which the Order Form and/or SOW states a "Total Recurring Fee" shall commence on the Billing Commencement Date and shall continue for the duration of the Term set out herein (the "Initial Term") unless otherwise terminated as set forth in this Agreement. Such Services shall automatically renew for additional successive terms of equal duration to the Term (the "Renewal Term") unless either Party delivers to the other Party written notice of its intention not to renew the Agreement no less than ninety (90) days prior to the expiration of the Initial Term or Renewal Term, as applicable.

3.3 Client's Termination with Cause. Notwithstanding anything to the contrary contained in this Agreement, Client may terminate this Agreement effective immediately upon delivery of notice of termination to Buffalo Computer Graphics if Buffalo Computer Graphics becomes insolvent or bankrupt or makes an assignment for the benefit of creditors or appoints (or having appointed) a receiver or trustee in bankruptcy or upon the proceeding in bankruptcy, receivership or liquidation being instituted against Buffalo Computer Graphics and continuing for thirty days without being dismissed.

3.4 Buffalo Computer Graphics' Termination with Cause. Notwithstanding anything to the contrary contained in this Agreement, Buffalo Computer Graphics may, at its option and in addition to any other rights and remedies available at law or equity, terminate this Agreement:

- a) any time during the Suspension Period for any reason upon prior notice to Client;
- b) upon written notice to Client if Client materially breaches this Agreement and such breach is incapable of cure or, with respect to a material breach capable of cure, Client does not cure such breach within thirty (30) days after receipt of written notice of such breach;
- c) immediately upon Client becoming insolvent or bankrupt or making an assignment for the benefit of creditors or appointing (or having appointed) a receiver or trustee in bankruptcy or upon any proceeding in bankruptcy, receivership or liquidation being instituted against Client and continuing for thirty days without being dismissed.

3.5 Payment Upon Termination and Effect of Termination. Upon providing notice of termination of this Agreement for any reason whatsoever (or termination of an Order Form or SOW) Client shall immediately pay to Buffalo Computer Graphics:

- (a) any accrued liability or amount owing for the Services rendered but not yet paid up to the effective date of termination in the case of termination of the applicable Order Form or SOW; and
- (b) any balance of Fees due to the end of the then current Term for the terminated Service(s).

Within five (5) business days of Buffalo Computer Graphics' receipt of all final Fees following termination or natural expiry of the Term, Buffalo Computer Graphics will make available to Client the Client Hardware (containing the Client Software, Custom Application (as applicable) and Client's data). Client acknowledges and agrees that Buffalo Computer Graphics is under no obligation to make available the Buffalo Computer Graphics Software and shall be allowed to remove it from the Client Hardware except in the case where the software is migrated to an on-premises solution pursuant to a written agreement between the parties.

Upon termination of this Agreement, any credits to which Client is entitled resulting from Buffalo Computer Graphics' failure to meet its SLA's in the last calendar month during the Term, shall be paid out to Client by Buffalo Computer Graphics within 60 business days of the effective date of termination of this Agreement. This Section shall survive the expiry or termination of the Agreement.

3.6 Service Suspension and Access Restriction. Buffalo Computer Graphics may suspend or restrict the Services (in whole or in part), including but not limited to the Service Levels (the "**Suspension Period**"):

- a) any time after the 60th day after the date of any invoice in the event that Client has not paid the subject invoice in full;
- b) at any time if Buffalo Computer Graphics' operations are impaired by Client's use of the Service(s);

Buffalo Computer Graphics will promptly recommence the Services following the cure of the underlying issue. Notwithstanding any suspension of Service(s), Client shall remain liable for payment of all invoices through the entire Suspension Period

4. Fees and Payment

4.1 Fees. "Fees" shall mean any one or more fee, as may be applicable as stated in the Order Form and/or SOW, and any other fees charged by Buffalo Computer Graphics. Fees include the cost of third-party retail services or products (including increases thereto) upon written notice to Client, purchased by Buffalo Computer Graphics at the request of Client. Any additional, supplemental or upgrade Services may result in additional fees or other charges. Client may request expedited service installation, and if Buffalo Computer Graphics is able to accommodate such request, Buffalo Computer Graphics may charge additional reasonable fees associated with such request. Client certifies that all information provided to Buffalo Computer Graphics is complete and accurate. Any costs incurred by Buffalo Computer Graphics due to errors or omissions documented on an Order Form of SOW (whether written or electronic) will be charged back to Client. Invoices will be emailed on a monthly or annual basis (depending upon agreed upon payment terms), in advance, to the email address listed in this Agreement, or to such additional or replacement email address(es) as directed by the Client. If no email is listed, invoices will be mailed to the address on the first page of this Agreement. Invoices are due within 60 days of the invoice date, except that Client may withhold from any payment any charge or amount disputed in good faith by Client pending resolution of such dispute. Fees shall be payable without counter-claim, setoff or demand. All Fees, invoices and payments shall be in US dollars unless otherwise stated.

4.2 Reduced Services. If Client subsequently selects a smaller quantity of or downgrades any of the Services before the end of the Initial Term or any Renewal Term, Client will remain responsible for paying all Fees and charges for such original quantity and level of Services to the end of the Initial Term or Renewal Term (as applicable). Client acknowledges that this Section 4.2 is not intended as a penalty clause and represents a genuine estimate of the losses that would be incurred by Buffalo Computer Graphics due to the reduction or downgrade of Service.

4.3 Credit. Buffalo Computer Graphics may at any time perform a credit analysis of Client. Client shall provide any credit information reasonably requested by Buffalo Computer Graphics. Following such credit analysis, Buffalo Computer Graphics may, in its sole discretion, require Client to pay the total Fees, or any portion thereof, in advance of providing Services and/or require other assurances to secure Client's payment obligations under this Agreement.

4.4 Taxes. In addition to the Fees, Client shall be responsible for paying any applicable sales, use, excise, value added or similar sales taxes or assessments imposed upon the Services by any federal, provincial/state, or local government authority, exclusive of taxes based upon Buffalo Computer Graphics' income or payroll.

4.5 Interest. Interest shall begin to accrue on unpaid invoices after thirty (30) days of the date of each invoice at the rate of the lower of 1.5% per month (18% per year) or the maximum permitted by law until paid in full.

4.6 Fee Increases and Renewal. Buffalo Computer Graphics may increase the Fees for any Renewal Term upon not less than 120 days' notice prior to the commencement of such Renewal Term. In addition, Buffalo Computer Graphics has the right to increase the Fees by the lesser of 2.5% of the preceding year's Fee or the percentage increase in the national Consumer Price Index over the prior twelve-month period. Notwithstanding the foregoing, Buffalo Computer Graphics may increase the Fees at any time immediately upon notice to Client in the event of industry changes, which are beyond the reasonable control of Buffalo Computer Graphics, including without limitation, carrier pricing policy changes, telecommunications tariff changes, commodity price increases and foreign exchange fluctuations.

4.7 Disputes. Subject to Section 4.2 of this MSA, Client may reasonably dispute any Fees if, and only if, Client:

- a) presents a written statement of any billing discrepancies to Buffalo Computer Graphics in reasonable detail together with appropriate supporting documentation no later than 5 days after notifying Buffalo Computer Graphics of such dispute; and
- b) negotiates in good faith with Buffalo Computer Graphics for the purpose of resolving such dispute within ten (30) days of submitting such written statement to Buffalo Computer Graphics. In the event such dispute is mutually agreed upon and resolved in favor of Client, Client will receive a credit for the disputed Fees. In the event the dispute is not resolved in such thirty (30) day period, either Party may pursue any available remedies.

4.8 Currency. All references to currency in this Agreement are to U.S. dollars, unless otherwise stated in the Order Form.

4.9 Service Levels; Credits. Refer to the Service Level Agreement exhibit for details on BCG's SLA. The remedies set forth in BCG's SLA constitutes Client's sole and exclusive remedy for BCG's failure to satisfy the commitments in the SLA.

Service credits, if any, as provided in the SLA or any other credits Client may be eligible to receive for Services purchased pursuant to a valid promotion will be issued to Client's account during the Term of the Agreement. In the case where there will be no further invoices, BCG will pay the amount of the service credits to Client in cash, by check or wire transfer, within 60 days after the end of the Agreement.

5. Representations, Warranties, Liability and Indemnity

5.1 Buffalo Computer Graphics Representations and Warranties. Buffalo Computer Graphics represents, warrants and covenants as follows:

- a) it has obtained all licenses, permits and approvals from any and all governmental authorities required in respect of its properties and operations as presently owned and carried on and in respect of the performance of the Services;
- b) to its knowledge, it is under no obligation or restriction, nor will it assume any such obligation or restriction, which would in any way interfere or be inconsistent with, or present a conflict of interest concerning the performance of the Services;
- c) it will perform its obligations hereunder in a professional and workmanlike manner and in accordance with applicable industry standards or as may be stated in an SOW or an Order Form;
- d) the performance of Services will not violate or infringe on the Intellectual Property Rights, proprietary rights, or any other rights, of any person;
- e) in carrying out its obligations under this Agreement, it shall comply with the terms and conditions of any applicable open source software license(s);
- f) it is a corporation duly incorporated under the laws of New York and is validly subsisting under such laws and has all the necessary corporate power and authority to own its properties and to carry on its businesses as presently owned and carried on;
- g) it has the corporate power and authority to enter into and perform its obligations under this Agreement; and
- h) it has duly authorized, executed and delivered this Agreement, and this Agreement constitutes a valid and binding obligation enforceable in accordance with its terms.

EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, BUFFALO COMPUTER GRAPHICS HEREBY DISCLAIMS AND MAKES NO WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR AVAILABILITY, LACK OF NEGLIGENCE, SERVICES OR THAT BUFFALO COMPUTER GRAPHICS EQUIPMENT WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT ALL ERRORS CAN OR WILL BE CORRECTED OR THAT THE SERVICES OR BUFFALO COMPUTER GRAPHICS'S EQUIPMENT WILL FUNCTION IN CLIENT'S ENVIRONMENT, OR LOSS OF DATA. BUFFALO COMPUTER GRAPHICS DOES NOT PROVIDE ANY WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, AND CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT, WITH REGARD TO THE EQUIPMENT OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) PROVIDED IN CONNECTION WITH THIS AGREEMENT. IN THE EVENT OF ANY INTERRUPTION, FAILURE OR BREAKDOWN IN THE SERVICES, OR OF THE LOSS OR SPOILING OF THE CONTENT, BUFFALO COMPUTER GRAPHICS MAKES NO WARRANTY THAT EITHER WILL BE RESTORED. UNLESS OTHERWISE STATED IN THIS AGREEMENT, THE CLIENT ASSUMES FULL RESPONSIBILITY FOR BACKING UP ITS OWN FILES AND THE ENTIRE RISK AS TO THE QUALITY OF, OR ARISING OUT OF, USE OR PERFORMANCE OF THE SERVICES AND BUFFALO COMPUTER GRAPHICS EQUIPMENT REMAINS WITH CLIENT. CLIENT EXPRESSLY ACKNOWLEDGES THAT ALTHOUGH BUFFALO COMPUTER GRAPHICS USES COMMERCIALY REASONABLE EFFORTS TO ENSURE THE PROTECTION OF CLIENTS DATA, BUFFALO COMPUTER GRAPHICS DOES NOT PROVIDE OR GUARANTEE ABSOLUTE SECURITY.

5.2 Client's Representations and Warranties. Client represents, warrants and covenants (where applicable) that:

- a) it is the true and lawful owner or licensee of the Client Software and Custom Applications (as applicable) and has the full right and ability to use such Client Software and Custom Applications as contemplated in this Agreement;
- b) it has the right to place Client Hardware in the Facility for receipt of the Services as contemplated herein;
- c) its use of Buffalo Computer Graphics controlled IP Addresses or use of the Services including any data transmitted, stored or received will not
 - (i) violate any applicable laws, regulations or Buffalo Computer Graphics Policies,
 - (ii) cause a breach of any agreement with any third party, or
 - (iii) interfere with other Buffalo Computer Graphics Client's use of any Buffalo Computer Graphics services or Buffalo Computer Graphics' network;
- d) it shall throughout the Initial Term and any Renewal Terms, be solely responsible and liable for the proper configuration, operation and management of the Client Software or Custom Applications (as applicable) without any liability, express or implied, accruing to Buffalo Computer Graphics whatsoever; and
- e) it has, where applicable, obtained all necessary consents to conduct its business in compliance with the *Personal Information Protection and Electronic Documents Act* or other similarly applicable federal or provincial/state statute.

5.3 Limitation of Liability.

Except for claims arising from Section 5.4, Section 5.5 or Section 6 of this MSA and any claims specifically exempted in any Terms and Conditions attached hereto, neither Buffalo Computer Graphics nor Client shall be liable to the other under the Agreement in connection with any single event or series of events for any special, indirect, consequential, exemplary or punitive damages including, but not limited to, lost profits, lost business revenue, lost or damaged data, failure to realize expected savings, or other commercial or economic loss of any kind even if the other Party has been advised of the possibility of these losses or damages, and regardless of the form of action, whether in contract or tort, including negligence or based upon any other legal or equitable theory. Furthermore, Client agrees that Client's sole and exclusive remedy for Buffalo Computer Graphics' failure to provide the Services in accordance with the applicable Service Levels shall be as set out in such Service Levels. Except for claims arising from Section 5.4, Section 5.5 or Section 6 of this MSA, and any claims arising out of BCG's gross negligence or willful misconduct, in no event will Buffalo Computer Graphics' liability to Client, or to that of its directors, officers, employees or users of the Services exceed the Fees actually paid to Buffalo Computer Graphics for the affect Service(s) within the three (3) month period immediately preceding the date on which the cause of action arose, excluding Fees for Implementation Services as itemized in Exhibit C. Notwithstanding the foregoing, BCG's total cumulative liability for claims arising from Section 5.4, Section 5.5 or Section 6 of the MSA, and any claims arising out of BCG's gross negligence or willful misconduct, will not exceed the total fees paid to Buffalo Computer Graphics for the affected Service(s) within the six (6) month period immediately preceding the date on which the cause of action arose.

5.3 Indemnity. Indemnity as related to this MSA is as follows:

- a) If either Party (the "Indemnitee") promptly notifies the other (the "Indemnitor") of a third party claim against the Indemnitee that any of the Services or Client supplied hardware, software or data, as the case may be, infringes a presently existing proprietary right of a third party, and if the Indemnitee specifies in such notice that the claim is based to any extent upon an alleged infringement of any portion of the Indemnitor's properties (Services or Client supplied hardware, software or data, as the case may be), the Indemnitor, with respect to and to the extent of the portion of the claim pertaining to the Indemnitor's properties, shall indemnify and defend such claim at its expense and pay any costs or damages that may be incurred or finally awarded against the Indemnitee. THIS SECTION SETS FORTH THE COMPLETE LIABILITY OF THE PARTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.
- b) Client agrees that it shall indemnify, defend and hold BCG, its officers, directors, employees and contractors harmless from and against any and all claims, costs, liabilities and damages which arise from or relate to the indemnifying Party's failure to comply in the conduct of its business with the CAN-SPAM Act of 2003 (15 U.S.C. 103) and the Telephone Consumer Protection Act and other similarly applicable federal or state statute(s).

- c) Client shall indemnify, defend and reimburse Buffalo Computer Graphics for, and hold Buffalo Computer Graphics harmless from, any and all claims or lawsuits of any person and resulting costs (including reasonable attorney's fees), damages, losses, consequences, awards and judgments:
 - i. for breach of Section 5.2 or Section 5.5 of this MSA;
 - ii. based on the use by Client or any third party of Content retrieved from or produced by the Services;
or
- d) In the event that either Party institutes any legal suit, action, or proceeding against the other Party arising out of or relating to this Agreement, the prevailing Party in the suit, action or proceeding shall be entitled to receive, in addition to all other damages to which it may be entitled, the costs incurred by such Party in conducting the suit, action, or proceeding, including reasonable attorneys' fees and expenses and court costs.
- e) An Indemnitee's failure to give prompt notice of a claim under this Section 5.4 shall not relieve Indemnitor of its obligation to indemnify except to the extent that Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. Indemnitor may not settle any claim pursuant to this Section 5.4 unless it unconditionally releases Indemnitee of all liability and does not include an admission of wrongdoing, fault or liability on behalf of Indemnitee.

This Section 5.4 shall survive expiry or termination of the Agreement.

5.5 Privacy. Each Party shall comply with all applicable privacy or data protection laws, statutes and regulations, including without limitation, having a written privacy policy governing the collection, use and disclosure of Personal Information (as such term is defined in the applicable statute) and being in compliance with such privacy policy. Without limiting the foregoing, BCG shall comply with the California Consumer Privacy Act of 2018 ("CCPA") and BCG shall process Client's personal information solely as necessary to provide the Services under this Agreement and as otherwise necessary to perform its obligations under this Agreement. BCG may only process Client's personal information for the duration of this Agreement. BCG acknowledges that it has given no consideration (monetary or otherwise) for any disclosure or transfer of Client's personal information from Client to BCG. Any such Client personal information is provided for the sole purpose of facilitating the Services. BCG shall comply with all reasonable documented instructions of Client with respect to Client's personal information, and shall immediately inform Client if, in BCG's opinion, an instruction conflicts with applicable data privacy laws. With respect to personal information as that term is defined by Section 1798.140 of the CCPA ("CCPA PI"), BCG will not collect, sell, or use the CCPA PI except as necessary to perform the purpose specified in this Agreement, and BCG will retain, use, or disclose CCPA PI only for the specific purpose of performing BCG's obligations under the Agreement and not for any other purpose, including selling, retaining, using or disclosing the CCPA PI for a commercial purpose other than providing the Services specified in or for the intended purpose of this Agreement.

BCG will not disclose, modify, or access Client's Data, except (a) with Client's authorization to do so in connection with Client's use of the Services, including requests for support; or (b) as necessary to provide the Services to Client or to prevent or address service or technical problems, or to comply with this Service Exhibit; or (c) at the request of a governmental or regulatory body, subpoenas or court order.

Based on the Services provided to Client by Buffalo Computer Graphics, Client grants permission to Buffalo Computer Graphics (which consent includes the initial installation and all future updates, patches, software and hardware configurations) to install the following on Client's application hosting platform provided by BCG and/or data hosting partner:

For Clients using Services that are managed by Buffalo Computer Graphics:

- a) anti-virus software installed for anti-virus also known as software for anti-malware protection. This software is used to prevent, detect and remove malicious software;
- b) monitoring software installed for the maintenance and observation of the performance of servers and server resources. This software will communicate securely with Buffalo Computer Graphics' centralized monitoring infrastructure;
- c) Buffalo Computer Graphics may install custom scripts and/or applications on Client's equipment or Buffalo Computer Graphics rental equipment in support or Buffalo Computer Graphics service maintenance and monitoring solution, or for other purposes by Client request. These scripts may create logs and send out e-

mails as required. The logs may be collected by Buffalo Computer Graphics and used for maintenance and troubleshooting purposes; and

- d) software and or agents to perform Client data backup and restoration functionalities.

BCG will store the Client Data only in North America, unless Client provides written authorization for an alternate location. BCG or its affiliates' personnel located outside of the United States shall not access the Client Data, except with Client's prior written consent.

5.6 No Control. Client acknowledges that Buffalo Computer Graphics does not own or have any control over the content, availability, accuracy or any other aspect of any information, data, files, pictures or content in any form or any type ("Content") made accessible or available by or to Client or Client's end users through the use of the Services and Buffalo Computer Graphics does not monitor the use of the Services by Client or its end users except as provided in this Agreement. Client agrees that all Content that Client accesses through Buffalo Computer Graphics is accessed and used by Client at Client's own risk, and that Buffalo Computer Graphics will not be liable for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to Client access to such Content.

In cases where BCG integrates with or provides third-party data Content, BCG does not have any control over the content, availability, accuracy or any other aspect of any information, data, files, pictures or content in any form or any type ("Content") made accessible or available by such third-party Content. In the event that there is an issue with accessing third-party services/data, BCG will work in good faith to resolve access issues.

5.7 BCG Compliance and Security. Buffalo Computer Graphics will comply with all laws and regulations applicable to BCG's provision of the Service, and Client will comply with all laws and regulations applicable to Client's use of the Service. BCG has adopted and implemented, and will maintain, a corporate information security program designed to protect Client data from loss, misuse and unauthorized access or disclosure. Such program includes formal information security policies and procedures. The BCG information security program is subject to reasonable changes by BCG from time to time. In addition to BCG's obligations in the Agreement, BCG, as of the date of this Agreement, has obtained an AICPA sanctioned Type II audit report (i.e., SSAE18/ISAE3402 SOC 1 or AT-101 SOC 2) for the hosting data centers and intends to continue securing such audits pursuant to a currently sanctioned or successor standard. Client, upon written request and under confidentiality agreement, will be entitled to receive a copy of the then-available report, which is BCG Confidential Information.

5.8 HIPAA. To the extent the Services involve the ongoing storage of or routine access to PHI (as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, "HIPAA"), or BCG is otherwise acting as a Business Associate (pursuant to HIPAA), BCG will agree to the terms in its then-current Business Associate Agreement upon Client's request.

6. Confidentiality

6.1 If applicable, an NDA shall apply to this Agreement and is hereby incorporated by this reference except that for the purposes of this Agreement the term of the NDA shall be extended until the end of the Initial Term (or Renewal Term as applicable) in the event that the NDA expires prior to the end of the Initial Term (or Renewal Term) of this Agreement.

6.2 In the event an NDA has not been executed by Client and Buffalo Computer Graphics, the Parties agree to hold in strictest confidence, not to use and not to disclose to any third party any Confidential Information of the other party, without the prior written consent of such other Party. For purposes of clarification, Buffalo Computer Graphics will not be prohibited or enjoined at any time from utilizing any skills or knowledge of a general nature acquired during the course of providing the Services, including, without limitation, information publicly known or available or that could reasonably be acquired in similar work performed for another Buffalo Computer Graphics client.

6.3 Unless otherwise prohibited by law, if the receiving party becomes legally obligated to disclose Confidential Information, the receiving party will give the disclosing party prompt written notice sufficient to allow the disclosing party to seek a protective order or other appropriate remedy, and will reasonably cooperate with the disclosing party's efforts to obtain such protective order or other remedy at the disclosing party's expense, and in the event the receiving party is unable to do so, the receiving party will (so long as not prohibited by law from doing so) advise the disclosing party immediately subsequent to such disclosure. The receiving party will disclose only such information as is required, in the opinion of its counsel, and will use commercially reasonable efforts to obtain confidential treatment for any Confidential Information that is so disclosed.

6.4 All Confidential Information will remain the exclusive property of the disclosing party, and the receiving party will have no rights, by license or otherwise, to use the Confidential Information except as expressly provided herein. Upon the disclosing party's written request, the receiving party will promptly return or destroy, and verify in writing its destruction of, all material, in any form, embodying Confidential Information of the disclosing party. In carrying out any destruction, the receiving party will protect Confidential Information in accordance with the terms of this Agreement.

6.5 The receiving party acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to the disclosing party for which monetary damages may be difficult to ascertain or be an inadequate remedy. The receiving party therefore agrees that the disclosing party will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

7. General

7.1 Provision of Public IP Addresses. Buffalo Computer Graphics will assign, on a temporary basis, a number of Internet Protocol Addresses ("IP Addresses") that Buffalo Computer Graphics, in its sole discretion, considers reasonable. Client acknowledges that

- a) IP Addresses are assigned as part of the Services and are not portable and
- b) Client does not obtain any right or title to assigned IP Addresses. Buffalo Computer Graphics reserves the right to change IP Address assignments at any time, provided Buffalo Computer Graphics uses reasonable commercial efforts to avoid disrupting the Services. Client agrees that any renumbering required of Client after termination of this Agreement shall be the sole responsibility of Client.

7.2 Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software.

- a) **Title.** Title to the Buffalo Computer Graphics Hardware and Buffalo Computer Graphics Software remains with Buffalo Computer Graphics or its suppliers, as the case may be and, except as expressly granted hereunder, no right title or interest in or to the Buffalo Computer Graphics Hardware or Buffalo Computer Graphics Software passes to Client. Accordingly, Client shall not dispose of or suffer a lien or encumbrance upon the Buffalo Computer Graphics Hardware or Buffalo Computer Graphics Software. Client further agrees to not
 - i. modify any part of the Buffalo Computer Graphics Software,
 - ii. translate, decompile, disassemble, decrypt, reconstruct, or reverse engineer the Buffalo Computer Graphics Software,
 - iii. remove any proprietary notices, labels or marks from the Buffalo Computer Graphics Software or Buffalo Computer Graphics Hardware,
 - iv. authorize or acquiesce in the use of the Buffalo Computer Graphics Software by persons other than Client and Buffalo Computer Graphics, and
 - v. copy the Buffalo Computer Graphics Software or documentation.
- b) **Leased Terms.** Client may not remove any item of Leased Hardware or Licensed Software from the Facility or Client location (whatever the case may be) and, unless otherwise agreed in writing by Buffalo Computer Graphics, may use the Leased Hardware and Licensed Software only for the purpose of delivering the Services. Buffalo Computer Graphics may replace items of Leased Hardware and accessories from time to time provided that it gives written notice to Client and that any such replacement does not substantially diminish the technical parameters of the Service. Buffalo Computer Graphics is not responsible for replacement of end of life hardware until support for such hardware is no longer available by the manufacturer, at which time replacement hardware will be as per manufacturer specifications. If any Leased Hardware or Licensed Software is damaged as a result of any act or omission of Client (including its agents, consultants or clients), Client shall compensate Buffalo Computer Graphics for the damage including any additional costs of repair incurred by Buffalo Computer Graphics.

7.3 Escalation Procedures. Buffalo Computer Graphics' current technical support escalation procedures are provided in the table below. All issues are responded to as quickly as possible in order to restore services and minimize downtime. BCG will work with the Client to determine the Severity and Impact of the reported issue based on the impact on business operation.

Problem Severity	Severity Code	Impact	Description and Resolution Support Requirement
1	Critical	Mission Critical	System is not operational/unavailable/significant measurable performance degradation: BCG will commit a full-time resource, or team of resources, to resolve the problem as soon as possible. All efforts will be made to resolve the issue within a twenty-four (24) hour period.
2	High	Major	Critical functionality is not operational: BCG will commit a full-time resource, or team of resources, during normal business hours to resolve the issue as soon as possible. All efforts will be made to resolve the issue with a forty-eight (48) hour period.
3	Medium	Moderate	Non-critical functionality is not operational: BCG will commit a resource, or team of resources, during normal business hours to restore service to a satisfactory level. All efforts will be made to resolve the issue within five (5) business days.
4	Low	Minor	Specific issue or questions exist but there is little or no impact to the organization's business operations: BCG will provide information or assistance during normal business hours as requested, and where possible. In most cases such assistance will be immediate, but where this is not possible, all efforts will be made to resolve the issue/question within twenty (20) business days.

Changes to the Escalation Procedures are subject to change at BCG's discretion; provided, however, that BCG will not reduce its obligations beyond the level set forth in this Agreement as of the Effective Date.

7.4 Buffalo Computer Graphics Policy/Product Guides. Buffalo Computer Graphics may, in its sole discretion, amend any of its information on its website, including without limitation, its policies and product guides, without notice to Client.

7.5 Technical Issues. Buffalo Computer Graphics may charge back all direct costs to Client associated with an investigation (at the request of Client) relating to a technical issue if Buffalo Computer Graphics concludes that the technical issue is not on its side or is not within the accepted number of support cases (or support window) covered by the Client's Maintenance & Support Package.

7.6 Monitoring. Buffalo Computer Graphics has no obligation to monitor Client's content or use of the Services. However, Client acknowledges and agrees that Buffalo Computer Graphics has the right to monitor content and Client's use electronically from time to time and to disclose any information as necessary to: satisfy any federal, provincial, local or international law, regulation or other governmental request or to do the following:

- a) assist in the pursuit of any legal action, including without limitation, actions against Client;
- b) operate Buffalo Computer Graphics' Services properly; and
- c) protect Buffalo Computer Graphics or its subscribers. Buffalo Computer Graphics reserves the right to either refuse to post or to remove any information or materials from the Services, in whole or in part, that Buffalo Computer Graphics decides, at its sole discretion, is unacceptable, undesirable, or in violation of this Agreement.

7.7 Insurance. Client shall, at its sole cost and expense, procure and maintain in full force and effect throughout the Term or Renewal Term (as applicable), such insurance as is reasonable in Client's industry, including, but not limited to, the following minimum coverages (with Buffalo Computer Graphics as an additional insured):

- a) all risk property insurance on any Client Hardware located at the Facility;

- b) Commercial General Liability insurance for bodily injury, property damage and loss of data in an amount not less than One Million Dollars (\$1,000,000.00) per occurrence;
- c) Workers' Compensation coverage in an amount not less than that prescribed by statutory limits; and
- d) Business Interruption insurance: Immediately upon commencement of the Services and thereafter upon Buffalo Computer Graphics' reasonable request, Client will provide certificates of insurance evidencing such coverage as set forth above. For greater certainty, Buffalo Computer Graphics will not provide insurance coverage for Client Hardware while located at the Facility.

7.8 Supported Browsers/Mobile Devices. Browser support is limited to mainstream browsers (e.g., Google Chrome, Apple Safari, Microsoft Edge, Firefox Mozilla) currently supported by their respective manufacturers (i.e., not deprecated or out of manufacturer support). Support of any browsers that land outside of manufacturer support is subject to additional fees. BCG reserves the right to drop support for any browser at any point during the life of the contract. BCG reserves the right to develop features that will only work in certain browsers even though browsers are covered by manufacturer support.

Browser Mobile support is limited to the latest iteration of the supported mobile platform (iOS and Android). BCG will not extend support to platforms that have been discontinued. Mobile browser support is limited to the primary Browser on the corresponding platform (Chrome on Android and Safari or Chrome on iOS).

8.0 Maintenance Window. Client acknowledges that the Services may be subject to routine maintenance or repair and agrees to cooperate in a timely manner and provide reasonable access and assistance as necessary to allow such maintenance or repair. Scheduled or emergency maintenance terms are identified in the SLA.

9.0 Product Lifecycle. This section refers to both the product as a whole and any modules, features, platforms, and technologies included within or supported by the Software.

9.1 Beta. Beta is defined as the period of time when a new product is tested by Client, but before it is generally available to the market. In preparation for Beta testing, Clients sign up and partner with the BCG development team for field testing. Beta Clients are key partners in validating that the product meets requirements and functions as set out in the product Documentation. During the Beta test period, Clients receive technical support and assistance from the development team.

9.2 General Availability. General Availability occurs when a product successfully completes the Beta period and becomes generally available to the market. This phase begins with a Product Announcement describing the application of the product. Regular releases are planned and full support is offered throughout the General Availability phase.

9.3 Continued Support. Continued Support is the phase a product enters as it approaches its End of Life. From time to time, it is necessary to discontinue a product for a variety of reasons, including lack of market demand, technology obsolescence or the availability of successor products. Once a product enters Continued Support, important milestones are communicated to our Clients throughout the phase. Continued Support for the Product is provided for a minimum of 12 months following the End of Life Announcement. No additional releases of the product are planned during this phase, and Continued Support for a product includes phone and online support. The End of Life Announcement will include an End of Sales date. On this date, the product is no longer available to be licensed, and is removed from the price list. Product support is provided to Clients who purchased a maintenance contract prior to the End of Sales date; maintenance agreements will not extend beyond the End of Life date.

9.4 Retired. Following retirement, support issues may be investigated, at Product Management's sole discretion, in an attempt to provide solutions or workarounds. BCG is under no obligation to provide support for a retired product unless the specific Client's contract expressly states otherwise

10.0 Publicity. BCG may use Client's name as part of a general list of clients. Each Party shall obtain the other Party's permission prior to using the other Party's name for any other marketing or promotional purposes. The Parties agree that any press release or other public comments issued by either Party relating to this Agreement will be prepared jointly between BCG and Client and will be issued upon mutual agreement of the Parties.

[Remainder of this page intentionally left blank]

IN WITNESS WHEREOF the Parties have executed this Agreement as of the date below. (Note: "Effective Date" is defined under the Composition of Agreement on the first page).

BUFFALO COMPUTER GRAPHICS, INC.

CLIENT

Signature

Signature

Name

Name

Title

Title

Date

Date

MASTER SERVICES AGREEMENT (MSA)
Exhibit A – Acceptable Use Policy

The Acceptable Use Policy sets forth the principles, rules, and regulations that govern the use by the Client of Buffalo Computer Graphics' networks, systems, services, and products. This Acceptable Use Policy has been established to promote the integrity, security, reliability, and privacy of Buffalo Computer Graphics' networks, systems, and Client data contained within. BCG may reasonably modify these policies to ensure compliance with applicable laws and regulations and to protect BCG's network and clients. BCG reserves the right to monitor (and suspend if applicable) processes on the (virtual) infrastructure to ensure Client compliance with this Agreement, including the AUP. Such monitoring does not include the monitoring or viewing of any Client Data. If BCG suspends Services for violation of this section, including the AUP, Client remains liable for all fees, charges and any other obligations incurred and accruing. No SLAs credits are payable for any period of suspension.

When using Buffalo Computer Graphics' networks, systems, products, and services the Client is prohibited from engaging in certain activities that include, but are not limited to, those described below. Such prohibited activities may, at the sole discretion of Buffalo Computer Graphics, be grounds for termination of Agreement with a Client, for the application of additional service charges or for the involvement of law enforcement agencies. Buffalo Computer Graphics reserves the right to remove any content or restrict the use of the Services for activities or content that in Buffalo Computer Graphics' reasonable judgment, violate the terms or conditions under which Buffalo Computer Graphics provides the Services or violate this Policy.

Indirect or attempted violations of the policy, and actual or attempted violations by a third party on behalf of a Buffalo Computer Graphics Client or a Client's end user, shall be considered violations of the policy by such Client. Buffalo Computer Graphics reserves the right to change the Policy by delivering notice of its decision to change the Policy to the Client at least 15 days prior to the changes taking effect. If you have any questions about this Policy, please contact Buffalo Computer Graphics at info@bcgeng.com.

Prohibited Uses of Buffalo Computer Graphics' Services and Products

This section of the Acceptable Use Policy identifies the uses and actions that Buffalo Computer Graphics considers in its reasonable judgment to be unacceptable and/or abusive, and thus, is strictly prohibited. The Client may only use Buffalo Computer Graphics' networks, systems, services and products in a manner that, in Buffalo Computer Graphics' sole judgment, is consistent with the purposes of such networks, systems, services and products. The following examples of prohibited uses and actions are non-exclusive and are provided for general guidance only.

1. to violate any law of any applicable jurisdiction, including, without limitation, laws governing advertising, alcohol, antitrust, child protection, drugs, encryption, exportation, food, financial services, firearms, gambling, importation, information systems, intellectual property, obscenity, privacy, securities, telecommunications and tobacco;
2. to commit a tortious or otherwise wrongful act, including, without limitation, the posting or communication of libelous, defamatory, scandalous, threatening, harassing, or private information without the permission of the person(s) involved, or posting content that is likely to cause emotional distress, whether through content, frequency, or size;
3. to engage in or to facilitate gambling activities;
4. to post, send, or receive any content that is obscene, pornographic, lewd, lascivious, or excessively violent;
5. to offer, solicit, sell, buy, rent, or license any goods, products, services, or information in, from, or to any location in which such activity is unlawful;
6. to advocate, promote, or otherwise encourage violence against any government, organization, group, individual or property, or to provide instruction, information, or assistance in causing or carrying out such violence;
7. to post, send, receive, display, distribute, or execute any content, including, without limitation, text, graphics, images, music, recordings, computer programs, links, frames, and "meta tags," that violates any copyright, right of publicity, patent, trademark, service mark, trade name, mask work, trade secret or other intellectual property right of others or use any tools designed to facilitate such access, such as packet "sniffers";
8. to delete or alter author attributions, copyright notices, or trademark notices, unless expressly permitted in writing by the owner;
9. to violate the terms of applicable software licensing agreements;
10. to obtain or attempt to obtain unauthorized access, such as attempting to circumvent or circumventing any authentication or other security feature of any system, network, or account. This includes accessing data not intended for the user, logging into a server or account the user is not authorized to access, or probing the security of any system, network, or account;
11. to interfere or attempt to interfere with service to any user, host, or network by use of any program, script, command, or otherwise. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service or to burden excessively a service's resources, and attempts to "crash" a host;
12. to introduce worms, harmful code and/or Trojan horses;
13. to attempt to circumvent the approval process for posting to a moderated newsgroup or bulletin board or to attempt to evade spam filters;
14. to cancel or supersede posts other than your own, with the exception of official newsgroup or bulletin board moderators performing their duties;
15. to send or post unsolicited messages or e-mail, whether commercial or not,
 - a) to any recipients who have requested that messages not be sent to them, or
 - b) to a large number of recipients, including users, newsgroups, or bulletin boards, at one time; or to collect responses from unsolicited email sent through the Services or from other external systems;
16. to send or post a message whose subject or content is unrelated to the subject matter of the newsgroup or bulletin board to which it is posted;
17. to send or post a message or e-mail with deceptive, absent, or forged header or sender identification information;
18. to propagate chain letters and pyramid schemes, whether or not the recipient wishes to receive such mailings;
19. to use Internet Relay Chat "bots";
20. to hold Buffalo Computer Graphics, its affiliates, officers, employees and/or shareholders up to public scorn or ridicule;
21. to resell Buffalo Computer Graphics' services, in whole or in part, to any entity or individual, without Buffalo Computer Graphics' prior written consent, or to misrepresent your relationship with Buffalo Computer Graphics
22. to forge, alter or remove header information or Client's identity;
23. to exceed any bandwidth caps or other limitations imposed by any of Buffalo Computer Graphics' underlying service providers;
24. to use the Internet in a manner that is not authorized by Buffalo Computer Graphics or its underlying service providers;
25. to operate a server in connection with Buffalo Computer Graphics or the Services for purposes other than for Client's normal business activity, including but not limited to mail, news, file, gopher, telnet, chat, web, or host configuration servers, multimedia streamers, or multi-user interactive forums; and/or
26. to use Buffalo Computer Graphics or the Services for operation of an ISP's business or for any other business enterprise in competition with Buffalo Computer Graphics.

Client is responsible for any misuse of the Services that it contracted for under this Agreement, even if the misuse was caused by its employee(s), contractor(s) or other third party(s) that had access to the Services. Client is responsible for ensuring that others do not gain unauthorized access to the Services. Client is solely responsible for obtaining, installing and maintaining all Client provided equipment and related services necessary to connect to Buffalo Computer Graphics' network. Client shall not connect or interconnect its equipment with any other equipment or services of any third party without Buffalo Computer Graphics' prior written consent and such consent shall not be unreasonably delayed or withheld. Client is solely responsible for the security of any device that Client connects to the Services, including any data stored on that device. In addition to Buffalo Computer Graphics' termination rights as set out in the Agreement, the Client engaging in one or more of these activities may result in, at the sole discretion of Buffalo Computer Graphics, acting reasonably, the suspension of Services (in whole or in part). Buffalo Computer Graphics may pursue any remedies available to it under the Agreement in the event of Client's breach of this AUP.

MASTER SERVICES AGREEMENT (MSA)

Exhibit B – Client Information Form

CLIENT CONTACT INFORMATION			
Legal Entity Name:			
Address:			
City:			
Province:		Postal code:	
Main Telephone:		Main Facsimile:	
HST#		PST Number?	
Email for notices:			
Email for invoicing:			

PRIMARY CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

BILLING CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

TECHNICAL CONTACT INFORMATION			
Contact Name:		Position	
Main Phone:		Cell Phone:	
Email Address:			
Alt Contact Name:		Alt. Contact Position:	
Alt Contact Name:		Alt. Contact Cell:	
Alt Contact Name:			

MASTER SERVICE AGREEMENT (MSA)

Exhibit C - BCG Managed Services Order Form/Statement of Work (SOW)

Quote Number:	
Project Manager / CSR:	
Client:	
Client Contact / PM (name):	
Client Contact (email):	
Client Contact (phone):	
Term:	
Term Start Date:	
Initial Term End Date:	
Annual Fee (excluding taxes):	
Onetime Fee (excluding taxes):	
Payment Terms:	
Billing Commencement Date:	
Services to be Provided:	
Client Responsibilities:	
Notes:	
Hosting Requirements:	
Hosting Data Center/Location:	
Terms & Conditions:	

BCG Signature

Client's Signature

Title

Title

Date

Date

MASTER SERVICES AGREEMENT (MSA)

Exhibit D – BCG Service Level Agreement

Updated 9/1/2020

This SLA is provided pursuant to and in accordance with the governing service agreement between Client and Buffalo Computer Graphics, Inc. The following Service Level Agreement (SLA) is applicable to the BCG Cloud Services Client for a fee and all credits are offered due to uptime guarantee failures. The SLA is not applicable to unrelated third parties or third parties lacking a contractual relationship with BCG. The uptime obligations and the resulting SLA credits are applied on a monthly basis unless specified otherwise in Exhibit E.

Public Network: BCG will deliver 99.9% uptime availability on all Public Network services to Clients located in BCG's Partner Cloud data centers. All Public Network services include redundant carrier grade Internet backbone connections, advanced intrusion detection systems, and denial of service (DOS) mitigation. This does not include DOS attacks or other unknown variables that can affect Internet traffic and are excluded from the issuance of SLA credits.

DisasterLAN (DLAN) Application: BCG will deliver 99.9% uptime availability on the DLAN Application. A DLAN Application failure occurs when a Client cannot access the DLAN Application because of problems with hardware and/or software in BCG's control. Access issues caused by problems connecting to the service, including without limitation problems on the Internet or access and configurations managed by a non-BCG provider, do not constitute failures and as such are not covered by this SLA. Clients will receive a service credit for the period of time commencing when a ticket is filed requesting assistance in accessing the DLAN Application and the access issue is verified by BCG until the services are reinstated.

Third Party Applications: BCG Cloud Services utilize a number of third-party services that are used to enhance content within BCG's base product including but not limited to AERIS weather, ESRI ArcGIS Online services, Microsoft Bing Services, and Google Map Services. These third-party services are not covered by BCG uptime availability guarantees and are out of BCG's control. While downtime related to these services will not affect BCG products directly in terms of overall functionality, it could result in these enhanced content offerings being unavailable at a time of need. Access issues related to these third-party applications do not constitute failures and are not covered by this SLA. Additionally, BCG makes no guarantees about the content or availability of services made available in BCG products via these third parties. Third party services are subject to the licensing terms of these said third parties and services offerings made by said third parties may be changed by the third party at any time. The modification, addition, or removal service offering from said third parties shall not constitute a breach in this SLA or any other agreement with BCG. Should said third parties make a change that may impact offerings available to the customer, BCG will notify the customer about such changes and offer alternative solutions if available. BCG will work in good faith to resolve any issues with third-party-provided data and services including the option to provide alternate data/service providers if necessary.

Simple Backup Service: BCG will perform nightly backups of application code and data and retain backups for 7 days.

Simple Disaster Recovery Service: BCG will provide an RPO time of 24 hours and an RTO time of 72 hours.

Maintenance: At certain times planned maintenance is required on the BCG Cloud that can cause service disruption. Maintenance services can affect the Public Network, Private Network, Virtual Servers, Cloud Storage, Security and other services. BCG will notify Client of planned maintenance service. BCG will provide at least 24-hour notice to Clients for potentially disruptive maintenance activity via email.

"**Emergency Maintenance**" refers to any corrective action intended to remedy conditions likely to cause severe Service degradation or correct critical security impacts, as designated by BCG in its sole discretion. Emergency Maintenance may include but is not limited to actions intended to address hardware or software failures or viruses/worms. BCG will exercise reasonable efforts to inform Client in advance before interrupting the Service for Emergency Maintenance, but such notice is not guaranteed and failure thereof does not constitute failure.

Support Response Time:

Note: The support details described in this section are applicable to BCG Cloud Services including the DLAN Application. BCG's standard business-day hours are 9 AM – 5 PM Monday-Friday (excluding holidays) Eastern Time. Clients can submit service-related issues at times in accordance with the terms of their contracted support tier (e.g., business day, 24/7/365).

Problem	Severity	Impact	Description and Resolution Support
---------	----------	--------	------------------------------------

Severity	Code		Requirement
1	Critical	Mission Critical	System is not operational/unavailable/significant measurable performance degradation: BCG will commit a full-time resource, or team of resources, to resolve the problem as soon as possible. All efforts will be made to resolve the issue within a twenty-four (24) hour period.
2	High	Major	Critical functionality is not operational: BCG will commit a full-time resource, or team of resources, during normal business hours to resolve the issue as soon as possible. All efforts will be made to resolve the issue with a forty-eight (48) hour period.
3	Medium	Moderate	Non-critical functionality is not operational: BCG will commit a resource, or team of resources, during normal business hours to restore service to a satisfactory level. All efforts will be made to resolve the issue within five (5) business days with either a fix or suitable workaround.
4	Low	Minor	Specific issue or questions exist but there is little or no impact to the organization's business operations: BCG will provide information or assistance during normal business hours as requested, and where possible. In most cases such assistance will be immediate, but where this is not possible, all efforts will be made to resolve the issue/question with either a fix or suitable workaround within twenty (20) business days.

Critical: Severity 1 Tickets receive a 30 minute time-to-acknowledge.

High: Severity 2 Tickets receive a 60 minute time-to-acknowledge.

Medium: Severity 3 Tickets receive a 1 business day time-to-acknowledge.

Low: Severity 4 Tickets receive a 1 business day time-to-acknowledge.

For all issues, Client must contact BCG support [via email at dlansupport@bcgeng.com or via phone] and create a ticket for which a tracking number will be provided and a support engineer assigned to review the support request within the timeframe listed above. If for some reason Client does not receive a response within the prescribed time intervals, Client should contact client care by phone and request that the support response be expedited.

BCG may reclassify any Ticket misclassified as falling into one of the Critical or High Priority categories listed above and such Ticket will not qualify for Critical or High Priority treatment.

Incident Reports: BCG will provide Client with an Incident Report via e-mail within seventy-two (72) hours for incidents resulting in greater than thirty (30) minutes of downtime. The Incident Report will include: incident date, duration, issue, details of the problem and details of the resolution.

SLA Credit Claim:

If a Client believes that a service failure occurred which occurs when the services are not available in accordance with this Agreement occurred, Client must open a support ticket (a "Ticket") by contacting BCG Support by email to dlansupport@bcgeng.com or via phone, and request any credits by accurately detailing the credit request within 30 days of the failure in question. BCG will issue to the Client appropriate service credits for the failure as defined in this SLA upon review and confirmation of the service failure.

Credit Limitations:

- 1) The minimum period of failure eligible for a credit is 15 consecutive minutes, and shorter periods will not be aggregated. The maximum credit shall not exceed one hundred percent (100%) of Client's fees for the affected Service feature for the then-current billing month. In the event that multiple periods of failure overlap in time, credits will not be aggregated, and Client will receive credit only for the longest such period of failure. In the event that a single incident calls for credits pursuant to multiple parts of this SLA, BCG will award credits for all Service features impacted in a single incident subject to the maximum credit noted above.

- 2) Credits available pursuant to this SLA will apply to future service delivery and will be credited against the applicable invoices. In the case where there will be no further invoices, BCG will pay the amount of the service credits to Client in cash, by check or wire transfer, within 60 days after the end of the Agreement.
- 3) Notwithstanding any provision to the contrary in this SLA, the following do not constitute failures:
 - a. downtime during planned maintenance (as defined above) or Emergency Maintenance (as defined below) periods;
 - b. outages caused by acts or omissions of Client that are prohibited by this Agreement;
 - c. outages caused by hackers, sabotage, viruses, worms or other third party wrongful actions if not detected by BCG's intrusion detection;
 - d. DNS issues outside of BCG's control;
 - e. outages resulting from Internet anomalies outside of BCG's control;
 - f. outages resulting from fires, explosions, or force majeure;
 - g. failures during a "beta" period;
 - h. any permissible suspension of Service pursuant to the Agreement;
 - i. during a time in which a Client is not in compliance with the AUP; or
 - j. the unavailability of required Client personnel, including as a result of failure to provide us with accurate, current contact information.

Exclusions:

- 1) This SLA provides Client's sole and exclusive remedies for any breach of the Service Levels set forth in this SLA.
- 2) This SLA does not cover (without limitation): (a) network performance to Client's physical location or Internet access point (such as a local DSL/cable modem); or (b) internal network issues or failures; or (c) failures due to denial of service attacks.
- 3) False or repetitive claims are subject to service suspension. Clients participating in malicious or aggressive Internet activities, thereby causing attacks or counter-attacks, do not qualify for SLA claims and shall be deemed in violation of the Acceptable Use Policy posted on the Website.
- 4) This SLA covers production-level servers and services, and does not apply to beta, sandbox, test, evaluation, training, or demo servers and services.

Credit Issued: For all SLAs, the service credit formula is as follows:

Hours of eligible downtime due to failure x Product and/or Service hourly cost = service credit.

- Credit Eligible Downtime due to failure = Time (in hours) past the SLA greater than 15 minutes excluding allowable downtime
- Product and/or Service hourly cost = Client's billing rate/hour during period of downtime of failure

MASTER SERVICE AGREEMENT (MSA)

Exhibit E – MSA/SLA Amendments

Revised 9/1/2020

The following outlined changes/additions to the BCG Master Services Agreement and/or SLA have been agreed upon by both BCG and the Client and supersede the corresponding respective Terms and Conditions outlined in the standard baseline MSA/SLA. Customer pricing shall reflect any additional fees necessary to provide the outlined changes/additions/upgrades.

- 1) **Hosting/Server Location(s)** – BCG will host the DLAN application and all respective data at one of our enterprise-class North American data centers provided by our hosting partner TBD.
- 2) **Concurrent Users** – System shall be architected and configured to support TBD concurrent users.

BCG Signature

Title

Date

Client's Signature

Title

Date