



NIMS STEP Evaluation Report

DisasterLAN version 7.4

March 2011



FEMA

DISCLAIMER: The evaluation results and use of trade names in this document do not constitute a DHS or FEMA certification or endorsement of the use of such commercial hardware or software.

Table of Contents

- Executive Summary 7
 - NIMS Concepts and Principles 8
 - Target Capabilities List 9
 - NIMS Technical Standards..... 10
- 1.0 Introduction 11
 - 1.1 Program Summary 12
 - 1.2 System Description 13
 - 1.2.1 Call Center..... 13
 - 1.2.2 Electronic Status Boards..... 14
 - 1.2.3 Administration Tools..... 15
 - 1.2.4 Planning..... 15
 - 1.2.5 Incident Folders 16
 - 1.2.6 Situation Reports 16
 - 1.2.7 Incident Reports 16
 - 1.2.8 GIS Information 16
 - 1.2.9 Streaming Video..... 16
 - 1.2.10 Contacting Others 16
 - 1.2.11 Reference Library Materials..... 17
 - 1.3 Objectives 17
 - 1.4 Evaluation Setup 18
 - 1.5 Evaluation Schedule..... 18
 - 1.6 Scope and Limitations..... 18
- 2.0 Execution..... 19

2.1 Participant Credentials	19
2.2 Methodology	19
2.2.1 NIMS Inspection and TCL Identification	19
2.2.2 NIMS Technical Standards Testing	20
2.3 Post-Assessment Activities	23
3.0 Results	24
3.1 NIMS Concepts and Principles	24
3.1.1 Objective 1: Inspect Incorporation of NIMS Concepts and Principles	24
3.2 TCL	35
3.2.1 Objective 2: Identify Applicable TCL Core Capabilities	35
3.3 NIMS Technical Standards	36
3.3.1 Objective 3: Determine Adherence to the CAP Standard	36
3.3.2 Objective 4: Determine Adherence to the EDXL-DE Standard	41
3.4 Participant Observations	45
4.0 Appendix A: National Incident Management System (NIMS) Criteria	53
4.1 Purpose	53
4.2 Instructions	53
4.3 Step 1 – Review the NIMS Criteria	54
4.4 Emergency Support	56
4.5 Hazards	57
4.6 Preparedness	57
4.7 Communications and Information Management	58
4.8 Resource Management	58
4.9 Command and Management	59
4.10 Other Criteria – Implementation and Product Overview	59

4.11 Step 2 – Apply NIMS Criteria and Complete NIMS STEP Worksheet	59
4.12 Step 3 – Address General Questions	59
4.13 NIMS STEP Worksheet.....	59
5.0 Appendix B: Target Capabilities List (TCL) Core Capabilities.....	61
6.0 Appendix C: References.....	63
7.0 Appendix D: List of Acronyms and Abbreviations.....	64

List of Figures

Figure 1: Tiered Evaluation Approach.....	12
Figure 2: Call Center Intake Screen.....	14
Figure 3: Status Board Screen.....	15
Figure 4: Local Weather	45
Figure 5: Sample Map Report.....	46
Figure 6: Sample Broadcast Message	47
Figure 7: Chat Header with Dropdown Selection List.....	48
Figure 8: Streaming Video.....	49
Figure 9: Resource Typing.....	50
Figure 10: Standard ICS Forms Menu	51
Figure 11: Call Center Call List.....	52

List of Tables

Table 1: NIMS Criteria Rating Summary	8
Table 2: Evaluation Objectives	17
Table 3: Evaluation Schedule	18
Table 4: Scope and Limitations	18
Table 5: Participant Credentials	19
Table 6: CAP Test Cases	20
Table 7: EDXL-DE Test Cases	22
Table 8: NIMS STEP Worksheet.....	26
Table 9: CAP Test Results	37
Table 10: CAP 1.1 Element Checklist Summary	39
Table 11: EDXL-DE Test Results	41
Table 12: EDXL-DE 1.0 Element Checklist Summary	43
Table 13: NIMS Criteria Rating Summary	54
Table 14: Minimum Product Requirements.....	55
Table 15: Core Target Capabilities Form	61

Executive Summary

This report presents the results from an evaluation of Buffalo Computer Graphics Incorporated's system¹ DisasterLAN 7.4 and is referred to throughout this document as DisasterLAN. This evaluation was managed by the Federal Emergency Management Agency (FEMA) and was conducted from 11 through 19 October 2010 as part of the National Incident Management System Supporting Technology Evaluation Program (NIMS STEP).

The type of evaluation performed for a system is dependant on the system's incorporation of National Incident Management System (NIMS) concepts and principles and/or NIMS recommended technical standards. This was a Comprehensive NIMS Evaluation; and therefore, it specifically addresses adherence to NIMS concepts and principles and one or more NIMS recommended technical standards. This evaluation had five objectives:

- **Objective 1** was to inspect the product's incorporation of NIMS concepts and principles.
- **Objective 2** was to identify the applicability of core capabilities recognized by the Target Capabilities List (TCL).
- **Objective 3** was to determine the system's adherence to the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) 1.1 standard.
- **Objective 4** was to determine the system's adherence to the OASIS Emergency Data Exchange Language-Distribution Element (EDXL-DE) 1.0 standard.
- **Objective 5** was to determine the system's adherence to the OASIS Emergency Data Exchange Language-Resource Messaging (EDXL-RM) standard. This was a pilot evaluation for EDXL-RM and reported separately in the NIMS STEP RM Pilot Evaluation Report DisasterLAN version 7.4 December 2010.

DisasterLAN is a web-based crisis management solution for use in any emergency operation center. DisasterLAN provides users with a toolset for managing incidents of any size. The system helps emergency managers with:

- Providing a formalized standardized documentation process
- Supporting both interagency and inter-jurisdictional communications and coordination
- Tracking and managing mission and asset requests
- Collecting, tracking and reporting on incident information and resources
- Developing and sharing a common operational picture
- Maintaining situational awareness

¹The terms product, system, and technology are used interchangeably throughout this report.

The NIMS STEP team used web browsers installed on NIMS Support Center workstations to access DisasterLAN. Participants logged into the system with vendor-provided usernames and passwords. The vendor provided user guides and conducted 14 hours of presentation, demonstration, and hands-on training. Evaluation activities were conducted on site at the Incident Management Test and Evaluation Laboratory (IMTEL).² Assessors with knowledge in the areas of emergency response and management conducted an inspection of the system, and provided a qualitative analysis and feedback on DisasterLAN based on concepts and principles from the NIMS document (December 2008). Assessors also identified which of the core capabilities from the TCL (September 2007) apply to the product. Engineers tested the system for adherence to the CAP and EDXL-DE standards.

NIMS Concepts and Principles

Table 1: NIMS Criteria Rating Summary provides a summary of findings for NIMS criteria. Key elements identified within each NIMS criterion are cited as Minimum Product Requirements. These requirements were derived from the NIMS document and impact the overall rating of the product’s adherence to NIMS concepts and principles. The numbers provided below summarize ratings (Agree, Disagree, Not Applicable) for Minimum Product Requirements within each NIMS criterion.

Table 1: NIMS Criteria Rating Summary

NIMS Criteria (Number of Minimum Product Requirements)	# Agree	# Disagree	# Not Applicable
Emergency Support (1)	1	0	0
Hazards (1)	1	0	0
Preparedness (1)	1	0	0
Communications and Information Management (9)	9	0	0
Resource Management (10)	10	0	0
Command and Management (2)	2	0	0

Note: A description of the NIMS criteria and Minimum Product Requirements is provided in [Appendix A](#).

DisasterLAN is consistent with all six of the NIMS criteria (Emergency Support, Hazards, Preparedness, Communications and Information Management, Resource Management, Command and Management). Overall, DisasterLAN applies to all of the 24 Minimum Product Requirements; of which 24 are consistent with NIMS concepts and principles. An overview for each NIMS criterion is provided below; explanations of all findings are provided in section [3.0 Results](#).

Emergency Support:

DisasterLAN meets the Minimum Product Requirement for Emergency Support as the system is consistent with applicable Emergency Support Functions (ESFs) and core functions of the Incident Command System (ICS). DisasterLAN applies to all of the 15 ESFs and it is applicable to all of the nine Incident Command functions (see Emergency Support in **Table 8: NIMS STEP Worksheet**).

² The laboratory is located within the Science Applications International Corporation’s (SAIC) Somerset, Kentucky facility.

Hazards:

DisasterLAN meets the Minimum Product Requirement for Hazards as the system can be used to plan for or respond to at least one hazard. The system applies to natural hazards, human- and technological-caused events.

Preparedness:

DisasterLAN meets the Minimum Product Requirement for Preparedness as the system can be used to support at least one of the core preparedness activities. DisasterLAN can be used to support planning, procedures and protocols, and training and exercises.

Communications and Information Management:

DisasterLAN meets all of the nine Minimum Product Requirements for Communications and Information Management. DisasterLAN provides on- and off-scene personnel access to critical information. The system has the capability to be updated continually in order to maintain situational awareness. The system is pre-loaded with ICS forms that users can complete on-line. DisasterLAN meets the SAFECOM Interoperability Continuum for data sharing via swapping files, common applications, custom-interfaces, one-way standards-based sharing, and two-way standards-based sharing. The system is scalable to support events of all sizes and adheres to the principle of plain language (clear text).

Resource Management:

DisasterLAN meets all of the 10 Minimum Product Requirements for Resource Management. The system addresses the need to manage resources and allows for the inventory of FEMA and non-FEMA typed resources.

Command and Management:

DisasterLAN meets all of the Minimum Product Requirements for Command and Management. The system is applicable to all of the 14 management characteristics of ICS.

Implementation Considerations:

It should take less than two weeks to implement DisasterLAN. The system's user guide is comprehensive and DisasterLAN's integrated help tool is intuitive. The system was reliable during the evaluation and it can enhance the user's ability to do his/her job.

Target Capabilities List

DisasterLAN applies to core capabilities that address: prevention, protection, response, recovery, and common capabilities. See [Appendix B](#) for a list of the core capabilities recognized by the TCL and [3.0 Results](#) for those capabilities that apply to the system.

NIMS Technical Standards

CAP

The test engineers determined that the system adheres with all required elements of the CAP standard. The test engineers successfully generated CAP alerts. The test engineers used two Extensible Markup Language (XML) validation tools to determine that the resulting messages were well formed and valid. The capability to send CAP alerts to Disaster Management Interoperability Services (DMIS) was verified. DisasterLAN implements all four segments of the CAP alert; there are a total of 13 required elements and 25 optional elements. DisasterLAN implements 100 percent of the mandatory elements, and 80 percent of the optional elements of the CAP standard.

EDXL-DE

The test engineer determined that the system adheres with all required elements of the EDXL-DE standard. DisasterLAN implements all three segments of the EDXL-DE message; there are a total of seven mandatory elements and 18 optional elements. DisasterLAN implements 100 percent of the mandatory EDXL-DE elements and 60 percent of the optional EDXL-DE elements.

1.0 Introduction

This report presents the results from an evaluation of Buffalo Computer Graphics Incorporated's system DisasterLAN 7.4. Evaluation activities are managed by FEMA's National Preparedness Directorate (NPD). The FEMA NPD provides strategy, policy, and planning guidance to build prevention, protection, response, and recovery capabilities among all levels of government throughout the nation. In support of this effort, the NIMS Support Center assists the responder stakeholder community with standards and technology integration, evaluations, exercises, and training activities relating to NIMS and preparedness. The NIMS Support Center is funded through the NIMS General Support Contract (NGSC) and managed by the Standards and Technology Branch of the National Integration Center (NIC) within FEMA. The program includes operation of a simulated Emergency Operations Center (EOC) with supporting technologies located at SAIC's facility in Somerset, KY.

As part of the NIMS Support Center, NIMS STEP provides an evaluation of commercial and government software and hardware³ products to assist in the implementation of NIMS. Evaluation activities are designed to expand technology solutions and provide the emergency response community with an objective process to evaluate their purchases. For more information on the evaluation program visit the [NIMS STEP website](#) or contact the [NIMS STEP team](#).

Products evaluated by NIMS STEP vary in system capabilities; therefore, NIMS STEP conducts four types of evaluations:

- Tier IV – Emergency Support Systems Evaluation
- Tier III – Comprehensive NIMS Evaluation
- Tier II – Technically Focused Evaluation
- Tier I – Comprehensive NIMS Evaluation with a Technical Component

Tier I products encompass Tier II – IV capabilities as these are systems used by emergency managers and responders during incidents/events that have clear ties to NIMS incident command and implement one or more of the NIMS technical standards. Definitions for each tier are provided in **Figure 1: Tiered Evaluation Approach**.

³ The term hardware is intended to relate specifically to products supporting the software under evaluation (e.g. sensors, cellular telephones, computer servers, etc.).

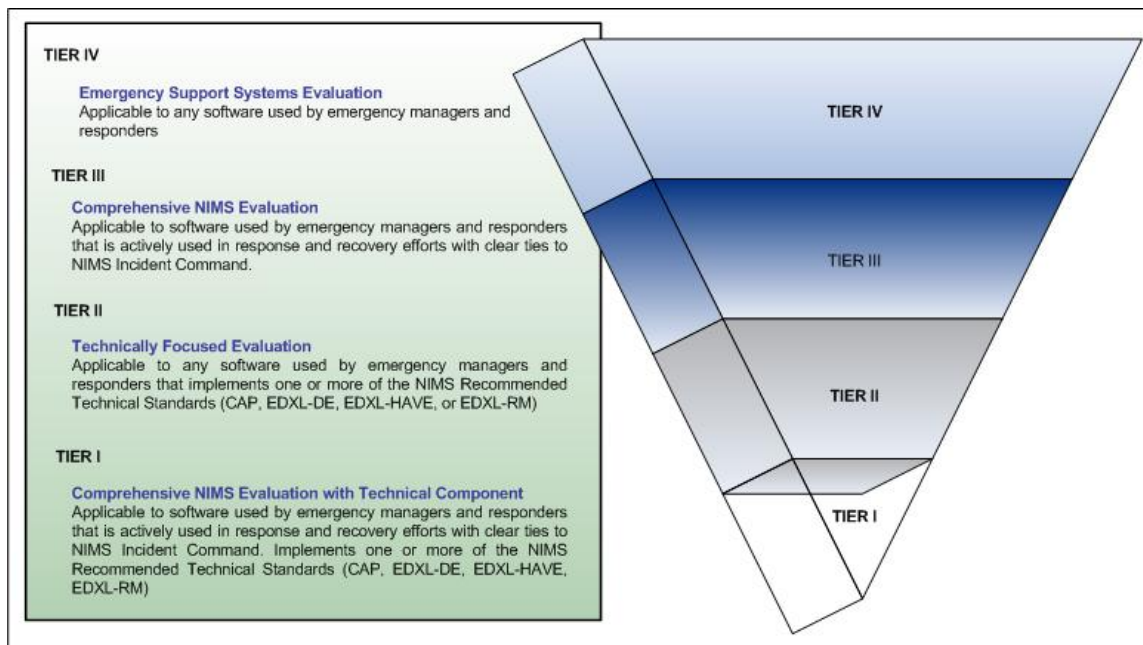


Figure 1: Tiered Evaluation Approach

A Tier I – Comprehensive NIMS Evaluation with a Technical Component was conducted for DisasterLAN. The intent of this evaluation was to determine the system’s ability to incorporate NIMS concepts and principles and applicable technical standards.

It is important to note that vendor participation in NIMS STEP is voluntary and the use of trade names and evaluation results in this document do not constitute a Department of Homeland Security (DHS) or FEMA endorsement or certification of the use of such commercial hardware or software. Evaluations do not constitute a determination of NIMS compliance.

1.1 Program Summary

NIMS provides a framework and sets forth, among others, the requirement for interoperability and compatibility to enable a diverse set of public and private organizations to conduct well-integrated and effective incident management operations. Systems operating in an incident management environment must be able to interact smoothly across disciplines and jurisdictions. Interoperability and compatibility are achieved through the use of tools such as common communications and data standards. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are the principal goals of the Communications and Information Management criterion of NIMS.

NIMS STEP evaluations primarily take place in a controlled, SEOC-based environment. However, some systems may require an additional or alternate environment, such as a limited field setting. In these cases, the field setting is considered an extension of the laboratory environment.

The IMTEL is accredited through the American Association for Laboratory Accreditation (A2LA). To achieve accreditation status, the laboratory was required to meet general requirements for the competencies of testing and calibration laboratories, as provided in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025:2005. Following the requirements outlined in ISO/IEC 17020:1998, the program leverages qualified assessors to inspect

products to determine if they follow established resource management and information management guidelines, among others. The current scope of accreditation and associated certifications are available on A2LA's website for [ISO/IEC 17025:2005](#) and [ISO/IEC 17020:1998](#). Results presented in [Section 3.1 NIMS Concepts and Principles](#) are within IMTEL's ISO/IEC 17020:1998 scope of accreditation; results presented in the [NIMS Technical Standards](#) section are within IMTEL's ISO/IEC 17025:2005 scope of accreditation. In the event that any individual findings fall outside their respective scopes of accreditation, they will be clearly annotated as such.



Evaluations take place usually over the course of four days during which the evaluation team, known as the NIMS STEP team, gains hands-on experience with the systems. The NIMS STEP team typically consists of one test engineer, one test analyst, and multiple assessors for each system under evaluation. The team is scaled appropriately based on the complexity and type of evaluation. Participants adhere to a non-disclosure agreement and a code of conduct which ensures objectivity and the protection of the vendor's sensitive information.

1.2 System Description⁴

DisasterLAN is a mobile or fixed site crisis management solution for use in any operation center. Emergency coordinators use personal computers or laptops that communicate via a web based interface with the DisasterLAN server. Once logged into DisasterLAN, users draw on any resources that they have been given access to. These resources include a Call Center for managing incoming requests, offers of assistance and reports; electronic status boards; administration tools; planning; incident folders; situation reports; incident reports; Geographic Information System (GIS) information; streaming video; and reference library materials. The primary resources are described in more detail below.

1.2.1 Call Center

Management of calls that come into an EOC is done by DisasterLAN's Call Center. This module provides a way to enter calls that have come into the EOC requesting resources; donating/offering resources; and reporting information. Calls can be routed to responsible parties, prioritized, marked with due dates and times, and have files and forms attached to them when appropriate. All call data is stored in the system for later analysis and management. Calls that are already entered into the system can be brought back up and edited at a later date. Coordinators can review outstanding calls and assign people and resources to address requirements. **Figure 2: Call Center Intake Screen** depicts the screen a call taker will enter information from a caller.

⁴ The vendor provided the majority of information within this section. Participants did not verify all of the system's capabilities during the evaluation, only those associated with the standards and criteria under test.

CALL REPRESENTS: Please Select Call Type
Ticket Number: Pending...

*Call Specifics

ABC Arial 12pt **A** **B** *I* U

Priority: Low Priority
Date/Time Due:

Status: New Call
Est. Completion Time:

Contact Information

Call Taker
File Attachments (0)

Caller Information

*Last:
*First:

Agency:

Address:

Country: United States of America
State: Kentucky

County: -- Select a State First --
Township: -- Select a County First --

Zipcode:

Coords: Coordinates Unknown

Primary: ext:
Contact 2: ext:

Contact 3:
Contact 4:

Email:

Notes:

Routings / Task Management
Associated Events / Incidents

Security Setting: Unrestricted

Figure 2: Call Center Intake Screen

1.2.2 Electronic Status Boards

The electronic Status Board takes the place of an EOC white or chalk board. It is used to dispense information to coordinators involved in an incident. This information can include such items as contact information, digital images, live weather data, DHS alert status, press briefings, and meeting data. The electronic Status Board can be displayed on a wall or screen at the EOC, but can also be assessable via web page to users connected to the system. **Figure 3: Status Board Screen** depicts the electronic Status Board that can be displayed in the EOC.

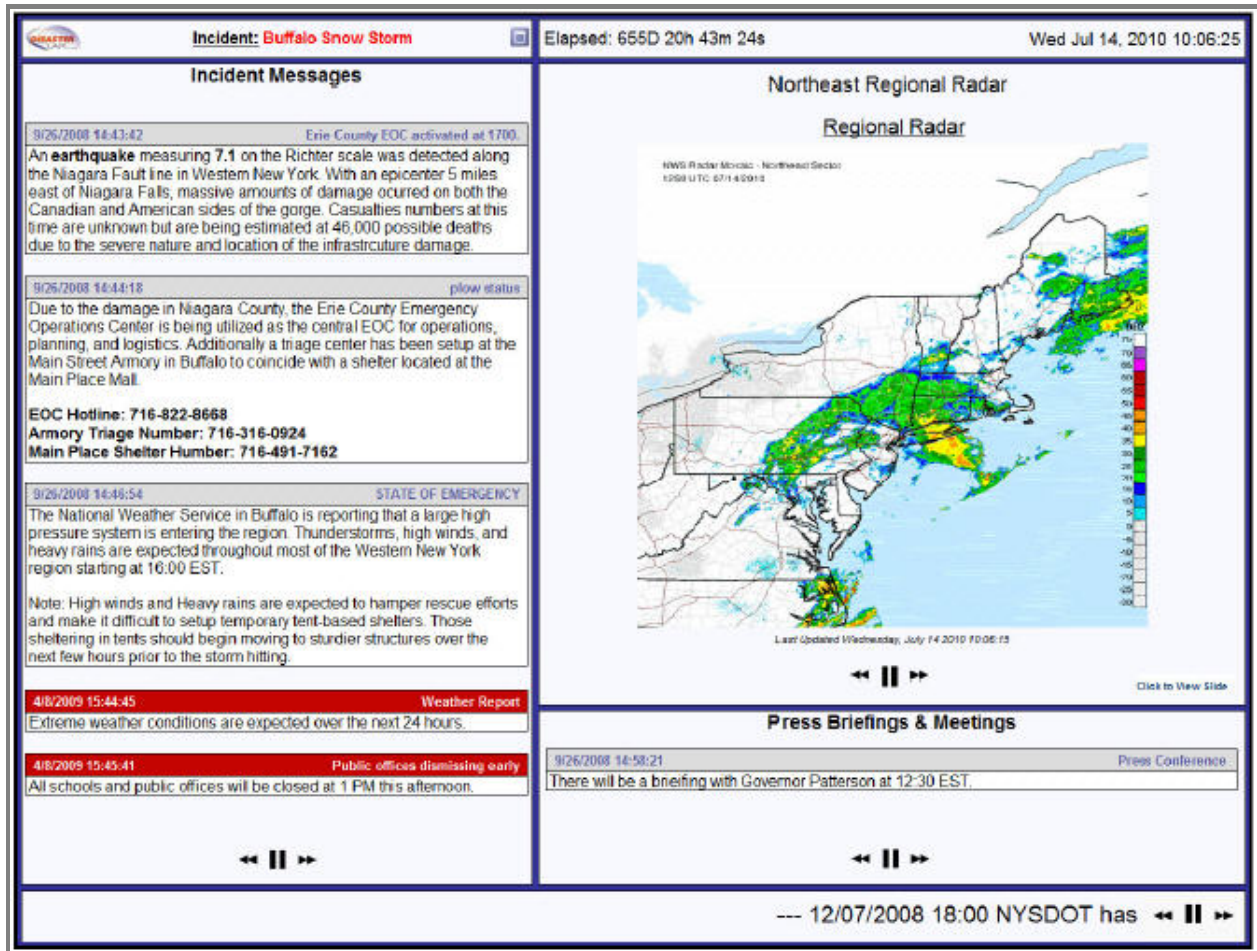


Figure 3: Status Board Screen

1.2.3 Administration Tools

Administration pages allow coordinators to produce reports on every call entered into the system. Statistics and graphs about call data can be generated to analyze where resources need to be concentrated. Administration pages also allow coordinators to dynamically change information on the Status Board, thus providing the ability to communicate information quickly to all emergency personnel. The Administration component of the system allows for specified personnel to control the security of each and every component available on the system. This provides coordinators with the ability to lock out particular components for users that do not need to access them.

1.2.4 Planning

The Planning module allows personnel and organizational information to be pre-loaded into the system. Personnel information that is stored in the system includes: names, addresses, contact numbers, and training records. Organization information that is stored in the system includes: type of organization (i.e. business, school, hospital, etc.), name, address, points of contact, and any special needs that might need to be provided for during an emergency.

1.2.5 Incident Folders

DisasterLAN Incident Folders include all documentation related to an incident. The helps coordinators locate documents, even after an incident has been closed. A default set of folders is created for each incident and new folders can be added as necessary to organize information effectively.

1.2.6 Situation Reports

Situation Reports in DisasterLAN allow collaborative reports to be compiled and published. Reports can be set up to be produced at periodic intervals, with custom headers and footers. This provides a way to gather information from various sources or agencies and produce reports for management, public dissemination or internal use.

1.2.7 Incident Reports

Incident Forms contain on-line copies of all Incident Command System (ICS) forms. Forms can be filled out and saved within each incident. The Incident Action Plan Module allows users to select the ICS forms that you want to include in your incident action plan, fill out common data in one place (which automatically flows down to selected forms) and then each form allows for form specific information to be entered. After completing all the forms, the Incident Action Plan can be published into a PDF file that is available for on-line review, distribution via e-mail, and is permanently saved with the incident creating a historic document.

1.2.8 GIS Information

DisasterLAN GIS capabilities include being able to demarcate an incident area on a map, geo-locate requests, offer and report using NIMS symbols, overlay Areal Locations of Hazardous Atmospheres (ALOHA) plumes to show projected areas that may be affected by release of toxic gas or other airborne pathogens, and pull up parcel data associated with areas underlying demarcation zones or plumes for affected people notification. DisasterLAN integrates with files created by an internal GIS department or with ESRI ArcWebServices. Map layer data includes topography, streets, location of shelters, schools fire hydrants, bridges, etc.

1.2.9 Streaming Video

DisasterLAN provides a Streaming Video Module that allows up to four simultaneous live video feeds to be displayed in the EOC and viewed by other coordinators logged into the system. Coordinators can utilize the Reference Library Module for a compilation of information on chemical, radiological and biological agents, on-line web-sites, and cached web-sites. Users can add local, state, and federal planning documents as necessary.

1.2.10 Contacting Others

This DisasterLAN module provides a variety of ways for contacting other people. The Incident Contacts list provides a list of all people who have been designated as key people involved in an incident. The Communications Center is used to send/receive messages from other DisasterLAN users and external

systems via CAP and EDXL protocols. The Chat Client module allows uninterrupted communication between system users.

1.2.11 Reference Library Materials

DisasterLAN comes preloaded with information on biological, chemical, and radiological agents; links to web-sites, cached web-site data, ICS forms, phone books, and preplanning documents. Additional documents specific to an organization can be uploaded into DisasterLAN's reference library.

1.3 Objectives

The NIMS STEP team developed a set of objectives to provide the foundation for this evaluation (see **Table 2: Evaluation Objectives**).

Table 2: Evaluation Objectives

Objectives
Objective 1: Inspect incorporation of NIMS concepts and principles.
Objective 2: Identify applicable TCL core capabilities.
Objective 3: Determine adherence to the CAP standard.
Objective 4: Determine adherence to the EDXL-DE standard.

Objective 1 addresses the incorporation of NIMS concepts and principles.⁵ This included a determination of how the system applies to the criteria for Emergency Support, Hazards, Preparedness, Communications and Information Management, Resource Management, and Command and Management. General questions on the system, including implementation considerations of the product were also addressed.

Objective 2 addresses the applicability of core capabilities recognized by the TCL. This included identification of capabilities that address prevention, protection, response, and recovery, as well as common capabilities such as planning and communications that support all missions.

Objective 3 addresses the implementation of the CAP standard, which is a format for exchanging all-hazard emergency alerts and public warnings. The CAP standard is on the NIMS Recommended Standards List. The NIC encourages implementation of the CAP standard in technology solutions.

Objective 4 addresses the implementation of the EDXL-DE standard which describes a standard message distribution framework for data sharing among emergency information systems using an XML-based format. The primary use of EDXL-DE is to identify and provide information to enable the routing of content. EDXL-DE messages can be targeted to geospatial or political target areas for message delivery. The EDXL-DE standard is on the NIMS Recommended Standards List. The NIC encourages implementation of the EDXL-DE standard in technology solutions.

⁵ All products are inspected for NIMS concepts and principles. The depth at which products are inspected for NIMS criteria depends on the type of evaluation conducted (e.g. a Comprehensive NIMS Evaluation [Tier III] or a Comprehensive NIMS Evaluation with a Technical Component [Tier I] is inspected in more detail for applicability to NIMS concepts and principles than is a Technically Focused Evaluation [Tier II]).

1.4 Evaluation Setup

The evaluation was conducted on site at the IMTEL. The vendor provided usernames/passwords for the web-based system. Test engineers managed the test environment, and were available to assist the vendor in resolving any technical issues.

1.5 Evaluation Schedule

The NIMS STEP team conducted the DisasterLAN evaluation from 11 through 19 October 2010. **Table 3: Evaluation Schedule** provides a summary of key events and milestones.

Table 3: Evaluation Schedule

Event	Date(s) 2010
Evaluation Readiness Review	1 October
Administrative system setup and pre-evaluation checks	8 October
Participant training	11 – 12 October
Rehearsal of system evaluation procedures	13 October
Evaluation execution	13 – 19 October
Data analysis and Quality Control (QC)	20 October

On 1 October, the NIMS STEP team conducted an Evaluation Readiness Review to ensure logistic and technical preparations were complete. The vendor provided participants with 2 days of on-site training (presentation, demonstration, and hands on) from 11 through 12 October. The participants evaluated the system on 13 through 19 October.

1.6 Scope and Limitations

Table 4: Scope and Limitations identifies issues that impacted the evaluation of DisasterLAN and the team's approach to mitigating them.

Table 4: Scope and Limitations

Limitation	Impact	Mitigation Strategy
None identified.		

2.0 Execution

2.1 Participant Credentials

Table 5: Participant Credentials summarizes the NIMS STEP team’s areas of expertise, role during the evaluation, and years of experience. In addition to personnel identified below, Information Technology (IT) personnel provide technical support during evaluations as necessary and they maintain IMTEL computer hardware and software.

Table 5: Participant Credentials

Current Title	Role	Years of Experience
Senior Systems Analyst	Emergency Response Assessor, NIMS Inspection (Experience: Firefighting, Technical-Heavy Rescue, Certified Emergency Manager)	35
External Assessor	Emergency Response Assessor, NIMS Inspection (Experience: Law Enforcement, Emergency Management)	35
Systems Engineer	Test Engineer	3
Systems Engineer	Test Analyst	17
Test Engineer	Test Engineer	17

2.2 Methodology

Assessors with knowledge in the areas of emergency response and management performed an evaluation for NIMS concepts and principles in a simulated operational environment. They also identified which of the core capabilities within the TCL apply to the product. A test engineer conducted an evaluation of the system’s adherence to the OASIS CAP 1.1 and EDXL-DE standards. The following sections describe the approach to the evaluation in more detail.

2.2.1 NIMS Inspection and TCL Identification

Prior to the inspection, assessors received scenarios from the vendor. Assessors reviewed and utilized two of these scenarios for use during the inspection (Flood and Snow Storm). Assessors also developed a customized scenario to be used during the inspection (School Shooting).

During the inspection, assessors documented their observations through the online Test and Evaluation (T&E) Data Collection System (DCS). Assessors also captured supporting screenshots.

2.2.1.1 NIMS Inspection

After using DisasterLAN, assessors completed a NIMS STEP Worksheet and provided qualitative feedback on the system based on concepts and principles from the NIMS. [Appendix A](#) provides a detailed description of the criteria used during the inspection. Assessors reviewed the system for applicability to the criteria Emergency Support, Hazards, Preparedness, Communications and Information Management,

Resource Management, and Command and Management. Assessors also reviewed general questions about the product including implementation considerations. Input from the assessors was captured using a dichotomous scale – a quantitative method for measuring the agreement or disagreement for a set of NIMS-related statements. The NIMS STEP team designed these methods to help describe systems and determine the presence or absence of desirable attributes. The NIMS STEP Worksheet results are provided in section [3.0 Results](#).

2.2.1.2 TCL Identification

After using DisasterLAN, assessors completed a TCL – Core Capabilities Form to identify the applicable core capabilities. [Appendix B](#) provides a list of the 37 capabilities recognized by the TCL that address prevention, protection, response, and recovery, as well as common capabilities. Input from the assessors was captured for measuring the agreement of the core capabilities applicable to the system. The TCL – Core Capabilities Form results are provided in section [3.0 Results](#).

2.2.2 NIMS Technical Standards Testing

2.2.2.1 CAP Test

The engineers executed the CAP test procedures, as identified in the DisasterLAN NIMS STEP Plan. There were a total of four test cases (see **Table 6: CAP Test Cases**). The engineers recorded objective findings, observations, and results for each test case. Additionally, for each test case, the test engineers assigned one of the following ratings: Meets requirements, no issues identified; Partially meets requirements, minor issues identified; Partially meets requirements, major issues identified; Does not meet requirements; No rating or not applicable. The test case, Transaction, received two ratings; one for sending and one for receiving. The test engineers documented their observations through the online T&E DCS.

Table 6: CAP Test Cases

Test Case Identifier	Test Case Title	Test Objective
TEST_CAP_001	Generate CAP Alert Message	Generate a CAP Alert message for use in the XML/Schema validation, CAP conformance, and transaction testing.
TEST_CAP_002	XML/Schema Validation	Determine if the message is well formed and valid against a CAP applied schema.
TEST_CAP_003	CAP Conformance	Determine if the system under test implements the CAP standard including cardinality of elements, mandatory and optional elements, with a focus on business and conditional rules.
TEST_CAP_004	Transaction	Verify transaction (send and/or receive) with disparate systems.

2.2.2.1.1 Test Case TEST_CAP_001 “Generate CAP Alert Message”

The objective of this test case was to generate a CAP alert message for use in test cases TEST_CAP_002 and TEST_CAP_003. The message contained one “alert” segment, one or more “info” segments, one or

more “resource” segments, and one or more “area” segments. The test engineers used all optional and mandatory fields that were available in the system to develop the CAP alert message.

2.2.2.1.2 Test Case TEST_CAP_002 “XML/Schema Validation”

The objective of this test case was to determine if the CAP alert message was well formed and valid against a CAP applied schema (CAP1_1Schema.xsd). The test engineers used the following software tools to complete this validation: XRay™2 XML Editor and an internally developed STEP Test Tool (STT).

2.2.2.1.3 Test Case TEST_CAP_003 “CAP Conformance”

The purpose of this test case was to determine if the CAP standard was applied in the correct format to include proper application of cardinality of elements, CAP standard structure, mandatory and optional elements and conditional rules. The test engineers used XRay™2 XML Editor to find elements within the XML CAP alert message generated in test case TEST_CAP_001. The test engineers checked for each element, as well as verified if the system permitted multiple or single entries for each of the elements as they are specified in the CAP standard. The test engineers used STT to supplement CAP conformance checks.

2.2.2.1.4 Test Case TEST_CAP_004 “Transaction”

The purpose of this test case was to verify transaction with a disparate system; a third party application or product (government or commercial). To successfully demonstrate transaction, the system under test must send and/or receive CAP messages (as applicable to the system) to a minimum of one disparate system (e.g., DMIS). The test engineers verified receipt and readability of a CAP alert message sent from DisasterLAN through the Open Platform for Emergency Networks (OPEN) and received by DMIS, and vice versa.

2.2.2.2 EDXL-DE Test

The engineers executed the EDXL-DE test procedures, as identified in the DisasterLAN NIMS STEP Plan. There were a total of four test cases (see **Table 7: EDXL-DE Test Cases**). The engineers recorded objective findings, observations, and results for each test case. Additionally, for each test case, the test engineer assigned one of the following ratings: Meets requirements, no issues identified; Partially meets requirements, minor issues identified; Partially meets requirements, major issues identified; Does not meet requirements; No rating or not applicable. The test case, Transaction, received two ratings; one for sending, and one for receiving. The test engineers documented their observations through the online T&E DCS.

Table 7: EDXL-DE Test Cases

Test Case Identifier	Test Case Title	Test Objective
TEST_EDXL-DE_001	Generate EDXL-DE Message Set	Generate an EDXL-DE message for use in the EDXL-DE XML/Schema validation, conformance, and transaction testing.
TEST_EDXL-DE_002	XML/Schema Validation	Determine if the message is well formed and valid against an EDXL-DE 1.0 applied schema.
TEST_EDXL-DE_003	EDXL-DE Conformance	Determine if the EDXL-DE standard is applied in the correct format to include proper application of cardinality of elements, EDXL-DE standard structure, mandatory and optional elements, and conditional rules.
TEST_EDXL-DE_004	Transaction	Verify transaction (send and / or receive) with disparate systems.

2.2.2.2.1 Test Case TEST_EDXL-DE_001 “Generate EDXL-DE Message Set”

The objective of this test case was to generate an EDXL-DE message set for use in test cases TEST_EDXL-DE_002 and TEST_EDXL-DE_003. Each EDXL-DE message set can consist of an <EDXLDistribution> element block, which may contain one or more <targetArea> and <contentObject> element blocks, of which a <contentObject> must contain either a <nonXMLContent> or <xmlContent> element block. The test engineers used all optional and mandatory fields that were available in the system to develop the EDXL-DE message.

2.2.2.2.2 Test Case TEST_EDXL-DE_002 “XML/Schema Validation”

The objective of this test case was to determine if the EDXL-DE message set was well formed and valid against an EDXL-DE applied schema (EDXL-DE_Schema_v1.0.xsd). The test engineers used the following software tools to complete this validation: XRay™2 XML Editor and STT.

2.2.2.2.3 Test Case TEST_EDXL-DE_003 “EDXL-DE Conformance”

The purpose of this test case was to determine if the EDXL-DE standard was applied in the correct format to include proper application of cardinality of elements, EDXL-DE standard structure, mandatory and optional elements, and conditional rules. The test engineers used XRay™2 XML Editor to identify elements within the XML EDXL-DE message set generated in case TEST_EDXL-DE_001. The test engineers checked for each element, as well as verified if the system permitted multiple or single entries for each of the elements as they are specified in the EDXL-DE standard. The test engineers used STT to supplement EDXL-DE conformance checks.

2.2.2.2.4 Test Case TEST_EDXL-DE_004 “Transaction”

The purpose of this test case was to verify transaction with a third party government product. To successfully demonstrate transaction, the system under test must send and/or receive EDXL-DE messages (as applicable to the system) to a minimum of one disparate system (e.g., DMIS). The test engineers verified receipt and readability of an EDXL-DE message set sent from DisasterLAN through OPEN and received by a disparate system, and vice versa.

2.3 Post-Assessment Activities

A test analyst was present during the evaluation and collected required data from all participants; the test analyst ensured data integrity and QC. The data collected during this evaluation included a collective NIMS STEP Worksheet, a collective TCL – Core Capabilities Form, completed test procedures, electronically submitted observation logs and spot reports, and screenshots and photographs. Data analysis began during the evaluation and resulted in the development of this evaluation report. After the evaluation was concluded, the NIMS Support Center conducted internal reviews of the report to ensure accuracy and completeness. The NIMS STEP team re-imaged IMTEL desktop systems.

3.0 Results

3.1 NIMS Concepts and Principles

3.1.1 Objective 1: Inspect Incorporation of NIMS Concepts and Principles

Following requirements outlined in ISO/IEC 17020:1998, qualified assessors inspected DisasterLAN to determine if the system incorporates NIMS concepts and principles, and documented results as identified in the following sections for Objective 1.

DisasterLAN is consistent with all of the six NIMS criteria; it is consistent with Emergency Support, Hazards, Preparedness, Communications and Information Management, Resource Management, and Command and Management.

3.1.1.1 *Emergency Support*

DisasterLAN applies to all ESFs and all Incident Command functions (Transportation; Communications; Public Works and Engineering; Firefighting; Emergency Management; Mass Care, Emergency Assistance, Housing, and Human Services; Logistics Management and Resource Support; Public Health and Medical Services; Search and Rescue; Oil and Hazardous Materials Response; Agriculture and Natural Resources; Energy; Public Safety and Security; Long-Term Community Recovery; External Affairs). DisasterLAN applies to all of the Incident Command functions (Incident Command, Operations, Planning, Logistics, Finance/Administration, Intelligence/Investigations, Public Information, Safety, and Liaison).

3.1.1.2 *Hazards*

The system applies to natural hazards, human and technological-caused events.

3.1.1.3 *Preparedness*⁶

DisasterLAN can be used to effectively support the preparedness activities for planning; procedures and protocols; training and exercises; personnel qualifications, licensure, and certification; equipment certification; and evaluation and revision.

3.1.1.4 *Communications and Information Management*

Common Operating Picture

DisasterLAN provides access to critical information. The system allows for on- and off- scene personnel to have the same information about the incident and it offers an incident overview by collating and gathering information that enables users to make effective decisions. The system has the capability to be updated continually in order to maintain situational awareness.

⁶ Preparedness was added in September 2010; it is currently not covered under the requirements outlined in ISO/IEC 17020:1998

Interoperability

DisasterLAN allows users to complete ICS forms. The system meets the SAFECOM Interoperability Continuum for data sharing via swapping files, common applications, custom-interfaces, one-way standards-based sharing, and two-way standards-based sharing.

Scalability

DisasterLAN can be used during small- and large-scale events and is flexible and scalable to support the full spectrum of multi-agency and multi-discipline incidents and events. The system applies to multiple levels of the government and to the public and private sector.

Plain Language

The system adheres to the principle of plain language (clear text).

Information Security

The system requires usernames and passwords to login and users are assigned roles/permissions. As a web-based system, security and vulnerability concerns are primarily tied to the Internet and not the product itself (e.g., loss of connectivity, hacking, viruses). According to the vendor, if a client chooses the vendor hosted option; all information on servers is encrypted.

3.1.1.5 Resource Management

DisasterLAN addresses the need to manage resources. The system allows for the inventory of FEMA and non-FEMA typed resources. The system identifies the use of mutual aid agreements but it does not specifically address the use of mutual aid resources. The system allows for personnel accounting and provides for a record of credentialed personnel.

3.1.1.6 Command and Management

DisasterLAN is consistent with all of 14 management characteristics of the ICS: Common Terminology; Modular Organization; Management by Objectives; Incident Action Planning; Manageable Span of Control; Incident Facilities and Locations; Comprehensive Resource Management; Integrated Communications; Establishment and Transfer of Command; Chain of Command and Unity of Command; Unified Command; Accountability; Dispatch/Deployment; Information and Intelligence Management.

3.1.1.7 Implementation and Product Overview

It should take less than two weeks for a department/agency to implement this system (from acquiring and installation to user proficiency). The system's user guide is comprehensive and DisasterLAN's integrated help tool is intuitive. The vendor offers online, train-the-trainer, on-site presentation and hands-on training. Training provided by the vendor is comprehensive and it allows recipients to proficiently use the system. Customer support is available 9:00 – 5:00 Eastern Standard Time (EST) by telephone or live chat. The size and makeup of a department or agency impacts time, resources, and funding associated with implementing the system.

DisasterLAN is intuitive and easy to use. The system was reliable during the evaluation and it can enhance the user’s ability to do his/her job. The primary capability of DisasterLAN is to allow an EOC to effectively manage a large scale disaster or pre-planned event.

3.1.1.8 NIMS STEP Worksheet

Table 8: NIMS STEP Worksheet provides specific details of the evaluation results.

Table 8: NIMS STEP Worksheet

EMERGENCY SUPPORT	
Criteria and Question	Result
EMERGENCY SUPPORT FUNCTIONS	
1. This product supports the following ESFs:	Agree/Disagree/Not Applicable
a. ESF #1 - Transportation	Agree
b. ESF #2 - Communications	Agree
c. ESF #3 - Public Works and Engineering	Agree
d. ESF #4 – Firefighting	Agree
e. ESF #5 - Emergency Management	Agree
f. ESF #6 - Mass Care, Emergency Assistance, Housing, and Human Services	Agree
g. ESF #7 - Logistics Management and Resource Support	Agree
h. ESF #8 - Public Health and Medical Services	Agree
i. ESF #9 - Search and Rescue	Agree
j. ESF #10 - Oil and Hazardous Materials Response	Agree
k. ESF #11 - Agriculture and Natural Resources	Agree
l. ESF #12 – Energy	Agree
m. ESF #13 - Public Safety and Security	Agree
n. ESF #14 - Long-Term Community Recovery	Agree
o. ESF #15 - External Affairs	Agree
2. There are no obstacles to ESF(s) implementing this product (i.e., from acquiring and installation to user proficiency).	Agree
3. Provide comments on ESF(s) implementing this product, including direct and indirect support.	The product is an extremely robust emergency management tool which supports all ESFs.
INCIDENT COMMAND	
4. This product supports the following Incident Command functions:	Agree/Disagree/Not Applicable
a. Incident Command	Agree
b. Operations	Agree

c. <i>Planning</i>	Agree
d. <i>Logistics</i>	Agree
e. <i>Finance/Administration</i>	Agree
f. <i>Intelligence/Investigations</i>	Agree
g. <i>Public Information</i>	Agree
h. <i>Safety</i>	Agree
i. <i>Liaison</i>	Agree
5. There are no obstacles to Incident Command functions implementing this product (i.e., from acquiring and installation to user proficiency).	Agree
6. Provide comments on Incident Command functions implementing this product, including direct and indirect support.	The product as demonstrated presented minimal obstacles for implementation. Any unique obstacles introduced by the product would be related to pre-loading data, additional hardware/software, specialized skill sets or resources.
7. This product is consistent with the applicable ESFs and core functions of ICS. (Minimum Product Requirement 1)	Agree
HAZARDS	
Criteria and Question	Result
8. This product can be used to plan for or respond to the following hazard types:	Agree/Disagree/Not Applicable
a. <i>Natural hazards</i>	Agree
b. <i>Human-caused events</i>	Agree
c. <i>Technological-caused events</i>	Agree
9. Provide comments on hazards applicability.	None identified.
10. This product can be used to plan for or respond to at least one hazard. (Minimum Product Requirement 2)	Agree
PREPAREDNESS	
Criteria and Question	Result
11. This product can be used to effectively support the following preparedness activities:	Agree/Disagree/Not Applicable
a. <i>Planning</i>	Agree
b. <i>Procedures and Protocols</i>	Agree
c. <i>Training and Exercises</i>	Agree
d. <i>Personnel Qualifications, Licensure, and Certification</i>	Agree
e. <i>Equipment Certification</i>	Agree
f. <i>Evaluation and Revision</i>	Agree

12. Provide comments on the product's support to preparedness activities.	The product is an emergency management tool which supports all preparedness activities.
13. This product can be used to support one or more core preparedness activities; a, b, or c above. (Minimum Product Requirement 3)	Agree
COMMUNICATIONS AND INFORMATION MANAGEMENT	
Criteria and Question	Result
COMMON OPERATING PICTURE	
	Agree/Disagree/Not Applicable
14. This product supports user access to critical information.	Agree
15. This product allows on-scene and off-scene personnel to have the same information about the incident (e.g., situational awareness).	Agree
16. This product offers an incident overview by collating and gathering information that enables the Incident Commander (IC), Unified Command (UC), and supporting agencies and organizations to make effective, consistent, and timely decisions.	Agree
17. This product has the capability to be updated continually in order to maintain situational awareness.	Agree
18. This product uses or interacts with geospatial information to portray the incident.	Agree
19. Provide comments on the common operating picture.	None identified.
INTEROPERABILITY	
	Agree/Disagree/Not Applicable
20. Incident reporting and documentation procedures are standardized to ensure situational awareness.	Agree
21. Comment on incident reporting and documentation procedures.	Reporting and documentation is done in a straightforward manner. Blank NIMS ICS forms are pre-loaded into the product for ease of use.
22. This product allows NIMS ICS forms to be completed.	Agree
23. If the product uses ICS forms, they remain consistent with the ICS form numbers and purpose of the specific type of form as identified by NIMS. (Minimum Product Requirement 4)	Agree
24. Provide comments on ICS forms.	None identified.

25. This product provides a method for data sharing or is interoperable with other incident management systems via voice, data, or video, etc. Identify the applicable level(s) of Data Elements interoperability on the SAFECOM Interoperability Continuum:	Agree/Disagree/Not Applicable
a. <i>Swap Files</i>	Agree
b. <i>Common Applications</i>	Agree
c. <i>Custom-Interfaced Applications</i>	Agree
d. <i>One-Way Standards-Based Sharing</i>	Agree
e. <i>Two-Way Standards-Based Sharing</i>	Agree
26. Provide comments on data sharing.	The product implements standards-based sharing for CAP and EDXL-DE as established by OASIS guidelines.
27. This product is interoperable with other systems at the level of c, d, or e above. (Minimum Product Requirement 5)	Agree
SCALABILITY	
	Agree/Disagree/Not Applicable
28. This product can be used to respond to small scale incidents and events. (Minimum Product Requirement 6)	Agree
29. This product can be used to respond to large scale incidents and events. (Minimum Product Requirement 7)	Agree
30. This product can be used by a single jurisdiction during incidents and events. (Minimum Product Requirement 8)	Agree
31. This product can be used across the full spectrum of multi-agency incidents and events. (Minimum Product Requirement 9)	Agree
32. This product can be used across the full spectrum of multi-discipline incidents and events. (Minimum Product Requirement 10)	Agree
33. This product allows responders to increase the number of users on a system.	Agree
34. Provide comments on scalability.	None identified.
35. The product can be used at the following:	Agree/Disagree/Not Applicable
a. <i>On scene as a portable or static device.</i>	Agree
b. <i>On scene at the Incident Command Post (ICP).</i>	Agree
c. <i>At a Staging Area, Base, or Camp.</i>	Agree
d. <i>At a local EOC.</i>	Agree
e. <i>At a state EOC.</i>	Agree
f. <i>At a Federal Joint Field Office (JFO) or EOC.</i>	Agree
36. Provide comments on Command and Coordination levels.	None identified.
37. This product can be used by the following levels of government:	Agree/Disagree/Not Applicable

a. <i>Municipality</i>	Agree
b. <i>County</i>	Agree
c. <i>Regional</i>	Agree
d. <i>Tribal</i>	Agree
e. <i>State</i>	Agree
f. <i>Federal</i>	Agree
g. <i>Special District</i>	Agree
h. <i>Agency</i>	Agree
i. <i>Other</i>	Agree
38. This product can be used to support communications among multiple levels of government(s).	Agree
39. Provide comments on levels of government.	None identified.
40. This product is flexible enough to be used by the public and private sectors.	Agree
41. Provide comments on use by the public and private sectors.	None identified.
PLAIN LANGUAGE	
	Agree/Disagree/Not Applicable
42. This product adheres to the principle of plain language (clear text). (Minimum Product Requirement 11)	Agree
43. Provide comments on the use of plain language.	None identified.
INFORMATION SECURITY	
	Agree/Disagree/Not Applicable
44. This product has redundancy capabilities as a part of its functionality.	Not Applicable
45. The product provides a means to properly authenticate and certify users for security purposes.	Agree
46. This product provides controls to restrict access to sensitive information. (Minimum Product Requirement 12)	Agree
47. This product does not introduce any unique security or vulnerability concerns.	Agree
48. Describe any safeguards integrated to minimize security and/or vulnerability concerns.	The system has the ability to lock any stored information. It provides security measures for user IDs and passwords. The system allows access to be determined at the level of a role or user ID.

<p>49. Provide comments on Information Security.</p>	<p>The following comments were noted as applicable to redundancy capabilities: In a hosted environment there is redundancy built into the vendor's infrastructure. In a self-hosted environment it would be the customer's responsibility to implement redundancy procedures. In the situation where the server is destroyed, the product provides the ability to produce hard copies of all information input into the system. There is an audit trail for every change that occurs within the system that infrastructure staff should be able to recover. According to the vendor, no information is ever truly deleted from the system.</p>
--	--

<p>Minimum Product Requirement Summary: Rating for the Communications and Information Management category.</p>	<p>Agree: 9 of 9 Disagree: 0 of 9 Not Applicable: 0 of 9</p>
---	---

RESOURCE MANAGEMENT

Criteria and Question	Result
	Agree/Disagree/Not Applicable
50. This product addresses the need to manage resources.	Agree
51. This product provides for requirements identification.	Agree
52. This product provides for mobilizing resources.	Agree
53. This product addresses the use of Mutual Aid Agreements and resources. (Minimum Product Requirement 13)	Agree
54. This product provides an integrated means for resource typing definitions. (Minimum Product Requirement 14)	Agree
55. This product provides a means for inventorying FEMA typed resources. (Minimum Product Requirement 15)	Agree
56. This product provides a means for inventorying non-FEMA typed resources. (Minimum Product Requirement 16)	Agree
57. This product provides a record of credentialed and other personnel. (Minimum Product Requirement 17)	Agree
58. This product provides a means for performing personnel and equipment accountability. (Minimum Product Requirement 18)	Agree
59. This product provides a means for resource requesting/ordering. (Minimum Product Requirement 19)	Agree
60. This product provides a means for resource tracking/reporting. (Minimum Product Requirement 20)	Agree

61. This product provides a means for resource recovery and demobilization. (Minimum Product Requirement 21)	Agree
62. This product assists in the reimbursement process. (Minimum Product Requirement 22)	Agree
63. Provide comments on resource management.	None identified.
Minimum Product Requirement Summary: Ratings for the Resource Management category.	Agree: 10 of 10 Disagree: 0 of 10 Not Applicable: 0 of 10
COMMAND AND MANAGEMENT	
Criteria and Question	Result
	Agree/Disagree/Not Applicable
64. This product assists users in the management of an incident.	Agree
65. This product supports (or is consistent with) the following management characteristics of ICS:	Agree/Disagree/Not Applicable
a. <i>Common Terminology</i>	Agree
b. <i>Modular Organization</i>	Agree
c. <i>Management by Objectives</i>	Agree
d. <i>Incident Action Planning</i>	Agree
e. <i>Manageable Span of Control</i>	Agree
f. <i>Incident Facilities and Locations</i>	Agree
g. <i>Comprehensive Resource Management</i>	Agree
h. <i>Integrated Communications</i>	Agree
i. <i>Establishment and Transfer of Command</i>	Agree
j. <i>Chain of Command and Unity of Command</i>	Agree
k. <i>Unified Command</i>	Agree
l. <i>Accountability</i>	Agree
m. <i>Dispatch/Deployment</i>	Agree
n. <i>Information and Intelligence Management</i>	Agree
66. Overall, this product is consistent with the applicable 14 ICS management characteristics. (Minimum Product Requirement 23)	Agree
67. If the product references ICS, the organization charts and/or terminology are consistent with it. (Minimum Product Requirement 24)	Agree
68. Comment on the product's integration of management characteristics of ICS.	None identified.
Minimum Product Requirement Summary: Ratings for the Command and Management category.	Agree: 2 of 2 Disagree: 0 of 2 Not Applicable: 0 of 2

IMPLEMENTATION AND PRODUCT OVERVIEW

Criteria and Question	Result
IMPLEMENTATION	
	Agree/Disagree/Not Applicable
69. This product can be easily implemented.	Agree
70. Comment on implementation.	Users should have equivalent ICS training for their respective positions.
71. System documentation (including training materials and user's guides) is comprehensive.	Agree
72. The vendor provides the following types of practitioner training:	Agree/Disagree/Not Applicable
a. <i>Online</i>	Agree
b. <i>Train the trainer</i>	Agree
c. <i>On-site presentation</i>	Agree
d. <i>Hands-on training</i>	Agree
73. Comment on practitioner training.	During the evaluation, real-time on-line assistance and training was successfully utilized.
74. Training provided allows recipients to proficiently use this product.	Agree
75. There are no unique obstacles introduced by this product that would prohibit a department or agency from providing product training.	Agree
76. Describe any unique obstacles to training.	None identified.
77. This product has an integrated help tool that is comprehensive.	Agree
78. Comment on the help tool.	The on-line help tool was easy to navigate and contained useful information.
79. Is customer support available? If so, what is its availability and what medium is used (e.g., e-mail, phone, live-chat)?	Standard customer support hours are from 9:00 am – 5:00 pm EST Monday-Friday. Customer service can be reached via telephone or live-chat. There is an opportunity to notify the vendor when a customer is working a disaster, allowing for extended customer service hours. Otherwise, extended coverage hours are available for an additional cost.
80. How long would it take a department, agency, or jurisdiction to implement this product?	Less than two weeks.

81. Comment on how the size or make up of a department, agency, or jurisdiction can impact the implementation of this product.	The implementation of the product is easily accomplished regardless of the department size.
82. Comment on any identified impacts.	None identified.
83. Federal, state, or local laws or regulations will not hinder the implementation of this product.	Agree
84. Comment on any laws that may hinder this implementation.	None identified.
85. Identify any issues with urban or rural implementation.	In a small organization it is straightforward to switch between different roles. In a large organization where each role is filled by one or more individuals it is easy to identify when the transfer occurs.
86. Identify any issues with paid, combination, or volunteer departments.	None identified.
87. Identify associated expenditures that may be incurred in addition to the initial procurement of this product.	The vendor provides updates to the product which are included in the annual maintenance fee. In a self-hosted environment additional costs could be incurred for hardware.
PRODUCT OVERVIEW	
88. Overall, this product is consistent with the concepts and principles of NIMS. To receive an agree in this category, this product must be consistent with all of the applicable supporting Minimum Product Requirements.	Agree
89. Identify any issues with NIMS consistency.	None identified.
90. This product will enhance the user's ability to do his/her job.	Agree
91. Comment on how this product will impact the job performance for the user.	The data collection and sharing, enhanced communications, and ease of access to information will aid any user in the performance of their job. It is configurable and easy to use. The use of NIMS ICS forms from the initial start-up of the incident to completion makes the reporting process simpler.
92. This product was easy to use and intuitive.	Agree
93. Comment on the products ease of use.	None identified.
94. This product was reliable during the evaluation.	Agree
95. Describe any issues with reliability.	None identified.
96. Comment on the primary capability/features provided by this product.	The product would enhance any EOC's management of a large scale disaster or pre-planned event.
97. Provide any other observations.	None identified.

3.2 TCL

3.2.1 Objective 2: Identify Applicable TCL Core Capabilities⁷

Assessors identified the following core capabilities as being applicable to DisasterLAN:

Common Capabilities:

- Planning
- Communications
- Community Preparedness and Participation
- Risk Management
- Intelligence and Information Sharing and Dissemination

Prevent Mission Capabilities:

- Information Gathering and Recognition of Indicators and Warning
- Intelligence Analysis and Production
- Counter-Terror Investigation and Law Enforcement
- Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Detection

Protect Mission Capabilities:

- Critical Infrastructure Protection
- Food and Agriculture Safety and Defense
- Epidemiological Surveillance and Investigation
- Laboratory Testing

Respond Mission Capabilities:

- On-Site Incident Management
- EOC Management
- Critical Resource Logistics and Distribution
- Volunteer Management and Donations
- Responder Safety and Health
- Emergency Public Safety and Security
- Animal Disease Emergency Support

⁷ Objective 2 was added in April 2010; it is currently not covered under the requirements outlined in ISO/IEC 17020:1998.

-
- Environmental Health
 - Explosive Device Response Operations
 - Fire Incident Response Support
 - Weapons of Mass Destruction (WMD) and Hazardous Materials Response and Decontamination
 - Citizen Evacuation and Shelter-in-Place
 - Isolation and Quarantine
 - Search and Rescue (Land-Based)
 - Emergency Public Information and Warning
 - Emergency Triage and Pre-Hospital Treatment
 - Medical Surge
 - Medical Supplies Management and Distribution
 - Mass Prophylaxis
 - Mass Care (Sheltering, Feeding and Related Services)
 - Fatality Management

Recover Mission Capabilities:

- Structural Damage Assessment
- Restoration of Lifelines
- Economic and Community Recovery

3.3 NIMS Technical Standards









3.3.1 Objective 3: Determine Adherence to the CAP Standard

Following requirements outlined in ISO/IEC 17025:2005, the qualified engineers tested DisasterLAN to determine if the system adheres to the CAP standard, and documented results as identified in the following sections for Objective 3.



Table 9: CAP Test Results provides a summary of key findings for the CAP test. The items shown in bold negatively impacted the rating in that area. The other items provided are observations.

The test engineers determined that the system adheres with all mandatory elements of the CAP standard and the majority of non-mandatory elements of the CAP standard. The test engineers were able to successfully generate CAP alerts. The test engineer used two XML validation tools to determine that the resulting messages were well formed.

Table 9: CAP Test Results⁸

Legend:				
 Meets requirements; no issues identified.  Partially meets requirements; minor issues identified.  Partially meets requirements; major issues identified.  Does not meet requirements.  No rating or not applicable to the system.				
Test Case Identifier	Test Case Title	Rating	Objective Results	Observations
TEST_CAP_001	Generate CAP Alert Message	 Meets requirements; no issues identified.	Successfully generated CAP messages.	The system made it easy for a user to create a CAP message by providing a well organized and comprehensive Graphical User Interface for entering information.
TEST_CAP_002	XML/Schema Validation	 Meets requirements; no issues identified.	Message well formed and valid.	
TEST_CAP_003	CAP Conformance	 Meets requirements; no issues identified.	Message adhered to all conformance requirements.	Pick list default values are configured by the system administrator. Fields allowed non-CAP conformance values to be entered.

⁸ The ratings and observations provided fall outside IMTEL's ISO/IEC 17025:2005 scope of accreditation. The legend ratings are subjective interpretations of the results.

TEST_CAP_004	Transaction (send)	 Meets requirements; no issues identified.	CAP messages are easily sent to DMIS using a pick list of addressee Collaborative Operating Groups (COGs). The system has the ability to send a plaintext message and the xml file at the same time.
TEST_CAP_004	Transaction (receive)	 Meets requirements; no issues identified.	CAP messages are automatically pulled by DisasterLAN from the DMIS COG account and show up in the system's external messages.

3.3.1.1 Mandatory and Optional CAP Elements

DisasterLAN implements all four segments of the CAP alert; a total of 13 mandatory elements and 25 optional elements. DisasterLAN implements 13 of 13 (100 percent) of the mandatory elements, and 25 of 31 (80 percent) of the optional elements. **Table 10: CAP 1.1 Element Checklist Summary** provides a summary of the CAP elements and identifies which elements are used by DisasterLAN. The elements that are mandatory per the CAP standard are shown in bold text.⁹ Each CAP Alert message consists of an “alert” segment, which may contain one or more “info” segments, each of which may include one or more “resource” and “area” segments.

There are six mandatory elements in the “alert” segment. The other three segments of the CAP alert are optional; however under most circumstances CAP messages with a message type value of “alert” should include at least one “info” segment. If a vendor chooses to implement an optional segment (“info”, “resource”, and/or “area”) then the supporting elements shown in bold text become required elements.

⁹ Elements in **bold** are mandatory; elements in *italics* have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted.

Table 10: CAP 1.1 Element Checklist Summary

Elements		Elements are used by the system under test		Elements sent by the system under test were received by the disparate system		Elements are used by the disparate system		Elements sent by the disparate system were received by the system under test		Comments (Note any discrepancies found)
		Yes	No	Yes	No	Yes	No	Yes	No	
alert Segment										
1.	Message ID (identifier)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.	Sender ID (sender)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.	Sent Date/Time (sent)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.	Message Status (status)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.	Message Type (msgType)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.	Source (source)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.	Scope (scope)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.	Restriction (restriction)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.	Addresses (addresses)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.	Handling Code (code) *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11.	Note (note)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.	Reference IDs (references)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
13.	Incident IDs (incidents)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
info Segment										
14.	Language (language)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
15.	Event Category (category) *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
16.	Event Type (event)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17.	Response Type (responseType) *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
18.	Urgency (urgency)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
19.	Severity (severity)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
20.	Certainty (certainty)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
21.	Audience (audience)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
22.	Event Code (eventCode) *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
23.	Effective Date/Time (effective)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	









Elements		Elements are used by the system under test		Elements sent by the system under test were received by the disparate system		Elements are used by the disparate system		Elements sent by the disparate system were received by the system under test		Comments (Note any discrepancies found)
24.	Onset Date/Time (onset)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
25.	Expiration Date/Time (expires)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
26.	Sender Name (senderName)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
27.	Headline (headline)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
28.	Event Description (description)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
29.	Instructions (instruction)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30.	Information URL (web)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
31.	Contact Info (contact)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32.	Parameter (parameter) *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
resource Segment		Yes	No	Yes	No	Yes	No	Yes	No	
33.	Description (resourceDesc)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
34.	MIME Type (mimeType)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
35.	File Size (size)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
36.	URI (uri)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
37.	Dereferenced URI (derefUri)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
38.	Digest (digest)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
area Segment		Yes	No	Yes	No	Yes	No	Yes	No	
39.	Area Description (areaDesc)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
40.	Area Polygon (polygon) *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
41.	Area Circle (circle) *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
42.	Area Geocode (geocode) *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
43.	Altitude (altitude)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
44.	Ceiling (ceiling)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

3.3.2 Objective 4: Determine Adherence to the EDXL-DE Standard



Following requirements outlined in ISO/IEC 17025:2005, the qualified engineers tested DisasterLAN to determine if the system adheres to the EDXL-DE standard, and documented results as identified in the following sections for Objective 4.

Table 11: EDXL-DE Test Results provides a summary of key findings for the EDXL-DE test. The items shown in bold negatively impacted the rating in that area. The other items provided are observations. The text engineers determined that the system adheres with all mandatory elements of the EDXL-DE standard.

Table 11: EDXL-DE Test Results¹⁰

Legend:				
 Meets requirements; no issues identified.  Partially meets requirements; minor issues identified.  Partially meets requirements; major issues identified.  Does not meet requirements.  No rating or not applicable to the system.				
Test Case Identifier	Test Case Title	Rating	Objective Results	Observations
TEST_EDXL-DE_001	Generate EDXL-DE Message Set	 Meets requirements; no issues identified.	Successfully generated EDXL-DE messages.	System allows user to easily create an EDXL-DE message with non-XML content by using an attachment feature.
TEST_EDXL-DE_002	XML/Schema Validation	 Meets requirements; no issues identified.	Message well formed and valid.	
TEST_EDXL-DE_003	EDXL-DE Conformance	 Meets requirements; no issues identified.	Message adhered to all conformance requirements.	

¹⁰ The ratings and observations provided fall outside IMTEL's ISO/IEC 17025:2005 scope of accreditation. The legend ratings are subjective interpretations of the results.

TEST_EDXL-DE_004	Transaction (send)	 Meets requirements; no issues identified.	EDXL-DE messages are easily sent to DMIS using a pick-list of addressee COGs. The system has the ability to send a plaintext message and the xml file at the same time.
TEST_EDXL-DE_004	Transaction (receive)	 Meets requirements; no issues identified.	System uses EDXL-DE to route the message and stores the information in the database. The system does not allow the user to view this information.

3.3.2.1 *Mandatory and Optional EDXL-DE Elements*

DisasterLAN implements all possible segments of the EDXL-DE message. Thus, there are a total of seven mandatory elements. DisasterLAN implements seven of seven (100 percent) of the mandatory elements and 15 of 25 (60 percent) optional elements. **Table 12: EDXL-DE 1.0 Element Checklist Summary** provides a summary of the EDXL-DE elements and identifies which ones DisasterLAN uses. The elements that are mandatory per the EDXL-DE standard are shown in bold text.¹¹ Each EDXL-DE message consists of an “EDXLDistribution” segment, which may include one or more “targetArea” and “contentObject” segments. The “contentObject” must include either XML or non-XML content. There are six mandatory elements in the “EDXLDistribution” segment.

¹¹ Elements in **bold** are mandatory; elements in *italics* have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted, # indicates conditional requirement.

Table 12: EDXL-DE 1.0 Element Checklist Summary

Elements		Elements are used by the system under test		Elements sent by the system under test were received by the disparate system		Elements are used by the disparate system		Elements sent by the disparate system were received by the system under test		Comments (Note any discrepancies found)
		Yes	No	Yes	No	Yes	No	Yes	No	
EDXL Distribution Element										
1.	distributionID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.	senderID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.	dateTimeSent	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.	distributionStatus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.	distributionType	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.	combinedConfidentiality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.	Language	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.	senderRole *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.	recipientRole *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.	keyword *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11.	distributionReference * #	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.	explicitAddress *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
targetArea Element (0..*)		Yes	No	Yes	No	Yes	No	Yes	No	
13.	circle *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
14.	polygon *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
15.	country *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
16.	subdivision *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
17.	locCodeUN *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
contentObject Element (0..*)		Yes	No	Yes	No	Yes	No	Yes	No	
18.	contentDescription	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	None directly related to the content

Elements		Elements are used by the system under test		Elements sent by the system under test were received by the disparate system		Elements are used by the disparate system		Elements sent by the disparate system were received by the system under test		Comments (Note any discrepancies found)
19.	contentKeyword *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	None directly related to the content
20.	incidentID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
21.	incidentDescription	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
22.	originatorRole *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
23.	consumerRole *	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
24.	Confidentiality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
25.	other *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
nonXMLContent Element		Yes	No	Yes	No	Yes	No	Yes	No	
26.	contentType	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
27.	Size	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
28.	Digest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
29.	Uri	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30.	contentData	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(or) XMLContent Element		Yes	No	Yes	No	Yes	No	Yes	No	
31.	keyXMLContent	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
32.	embeddedXMLContent	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

3.4 Participant Observations

Participants noted the following observations during the evaluation:

System Capabilities

- The DisasterLAN Weather module allows users to display local, national or tropical weather.

Figure 4: Local Weather depicts the current local weather conditions for New York, New York.

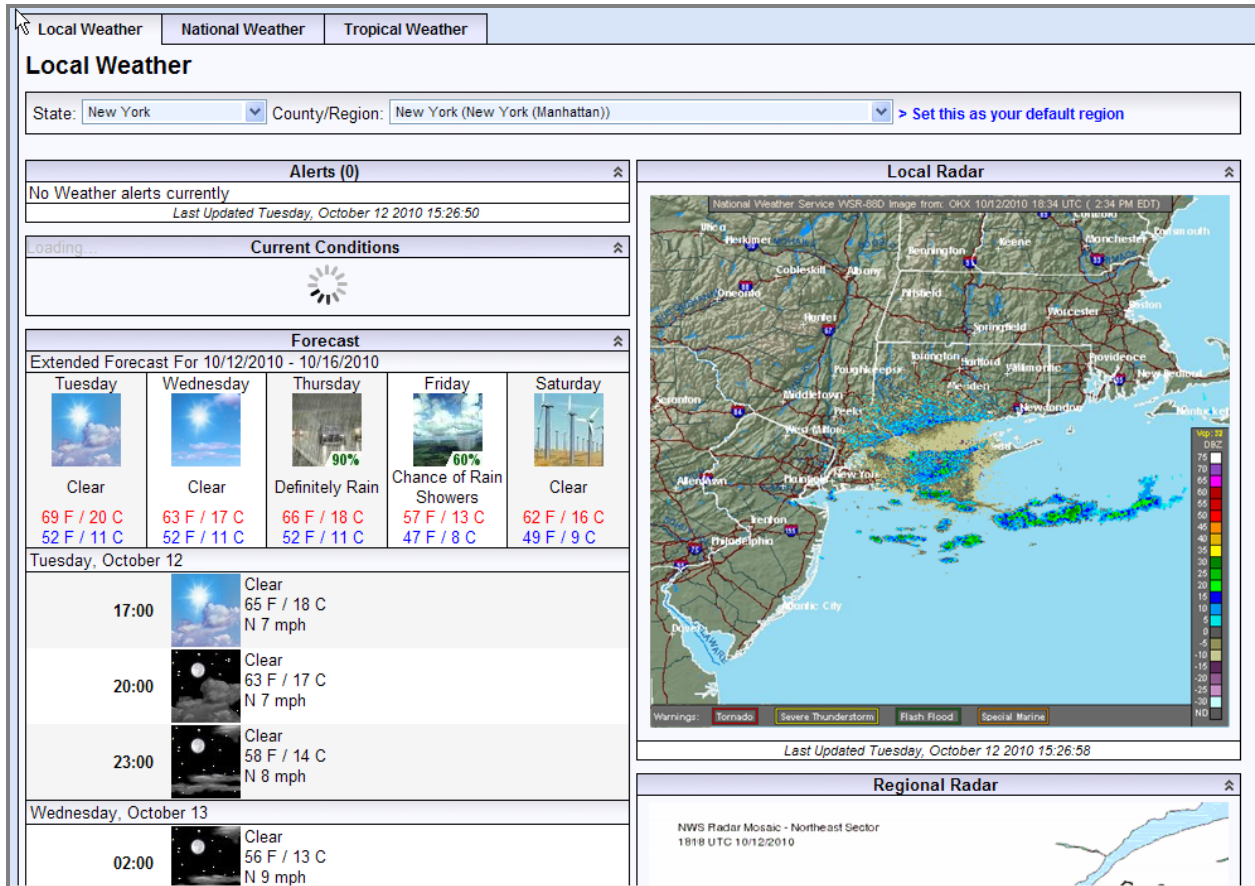


Figure 4: Local Weather

- After an incident, the Incident Management Mapping module can be used to produce a map of the incident, creating the basis for historic and legal documentation. **Figure 5: Sample Map Report** depicts an after incident map report.

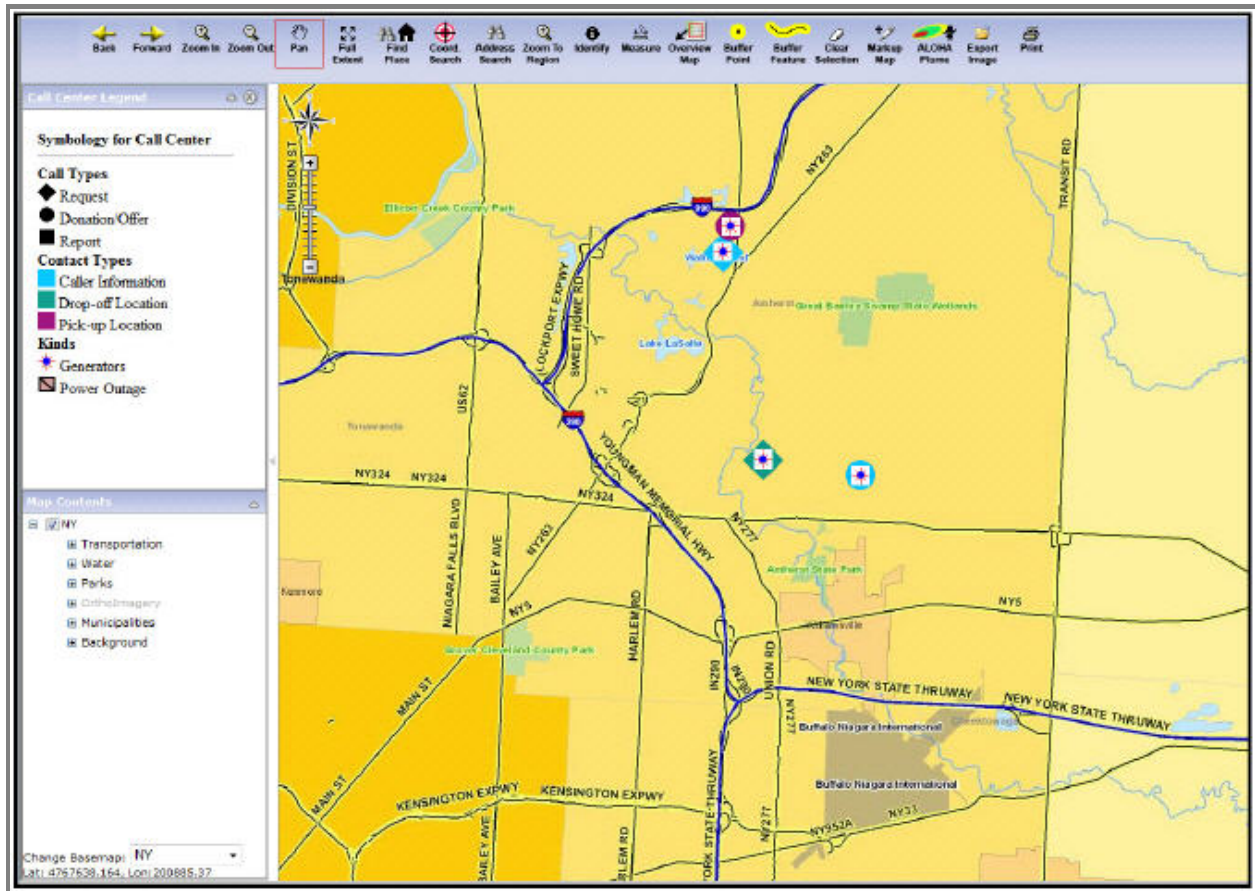


Figure 5: Sample Map Report

- The Reference Library contains information on various emergency related documents such as emergency plans, chemical reference guide, biological agent fact sheets, etc. Material in the Reference Library can be customized so that it includes the documents needed during emergency or non-emergency situations. The following categories of information are typically included with the baseline DisasterLAN Reference Library:
 - Biological Agents
 - Chemical Agents
 - ICS Forms
 - Federal/United States Emergency Contact Numbers
 - Phone Books
 - Preplanning Documents
 - Radiological Agents
 - Web-Sites (online and cached off-line)

Information Sharing

- DisasterLAN provides multiple ways of sharing information. One method to share information is to send a broadcast message. **Figure 6: Sample Broadcast Message** is an example of the Broadcasts information screen displayed within the Communications Center.

The screenshot displays the DisasterLAN interface. At the top, it shows 'Incident: Buffalo Snow Storm' and the user's role as 'BCG Support Staff (JT)'. The date and time are 'Tue Jul 13, 2010 17:29:56'. The interface includes a navigation sidebar on the left with options like 'Mailbox', 'DMail', 'Broadcasts', 'External Messages (2757)', 'External Calls', 'Sent Items', 'Sent Internal Messages', 'Sent External Messages', 'Chat', and 'History'. The main area shows a list of broadcast messages with columns for 'From', 'Subject', 'Incident', and 'Received'. The selected message is from 'User Demonstration (DemonstrationUser)' with the subject 'Information Update to All EOC' and is dated '7/13/2010 17:27:48'. Below the list, there are action buttons: 'Delete', 'Edit', 'Print', and 'Full View'. The message content reads: 'Information Update to All EOC Staff', 'Received: 7/13/2010 5:27:48 PM', 'From: User Demonstration (DemonstrationUser)', 'Incident: Buffalo Snow Storm', and 'The Governor's Office has expanded the Emergency Declaration to include Niagara and Orleans Counties. Please have Agency Liaisons begin contacting their support for those areas.'

Figure 6: Sample Broadcast Message

- A method of communicating during an incident is chatting with online users via DisasterLAN's online chat. **Figure 7: Chat Header with Dropdown Selection List** depicts how a user can see which users are online and are available for chat.

The screenshot displays the DisasterLAN web interface. At the top, the incident is identified as 'Incident: Buffalo Snow Storm' with the date 'Tue Jul 13, 2010 17:46:49'. The user is logged in as 'demonstrationuser'. A dropdown menu titled 'Online Users' is open, listing several users including 'bcg', 'Clohessy, James (bcg_jclohessy) - BCG Support Staff (IT)', 'Demonstration, User (DemonstrationUser) - BCG Support Staff (IT)', 'Kensy, Nancy (bcg_nancyLR) - EOC Manager', 'Marciniak, Rob (bcg_rmarciniak) - Agency - Department of Health (DOH)', and 'meinhart, ken (bcg_kmeinhart) - Agency - Department of Health (DOH)'. To the right, a 'Menu' is visible with various options like 'Assets or support, and informational reports', 'er requests, offers, and informational reports', 'requests, offers or informational reports', 'statistics module', 'Duty Officer Module', 'Contact information for key individuals involved in mitigating this incident', 'Directory of all users who have DisasterLAN accounts', 'Communication Center', 'Briefing Notes / SSF Logs', 'Electronic Status Board containing up to date incident information, messages, weather, and photos', 'Streaming video from select streaming video feeds', 'Weather bulletins & radar imagery', 'DisasterLAN's Geographic Information System', 'Organizations, personnel, organizational needs & resources', 'Calendar for scheduled meetings and events', 'Incident Command System (ICS) Forms', 'Incident Action Plans', 'Situation Reports (Standard)', 'Incident related documents', 'Reference documents, response plans, and on-line & off-line web sites', 'View your user profile, edit information or change your password', and 'System management & administration including site security'.

Figure 7: Chat Header with Dropdown Selection List

- With DisasterLAN's Streaming Video Module, video from traffic cameras, weather cameras or cameras located at an incident scene can be displayed in the EOC using a video projector. Anyone using DisasterLAN can view streaming video on the computer screen. When you select Streaming Video from the Main Menu, a pop-up screen with four view panels appears. Each panel contains a video selector drop-down menu that allows the user to select the camera they want to view. An example of the steaming video viewer is shown in **Figure 8: Streaming Video**.

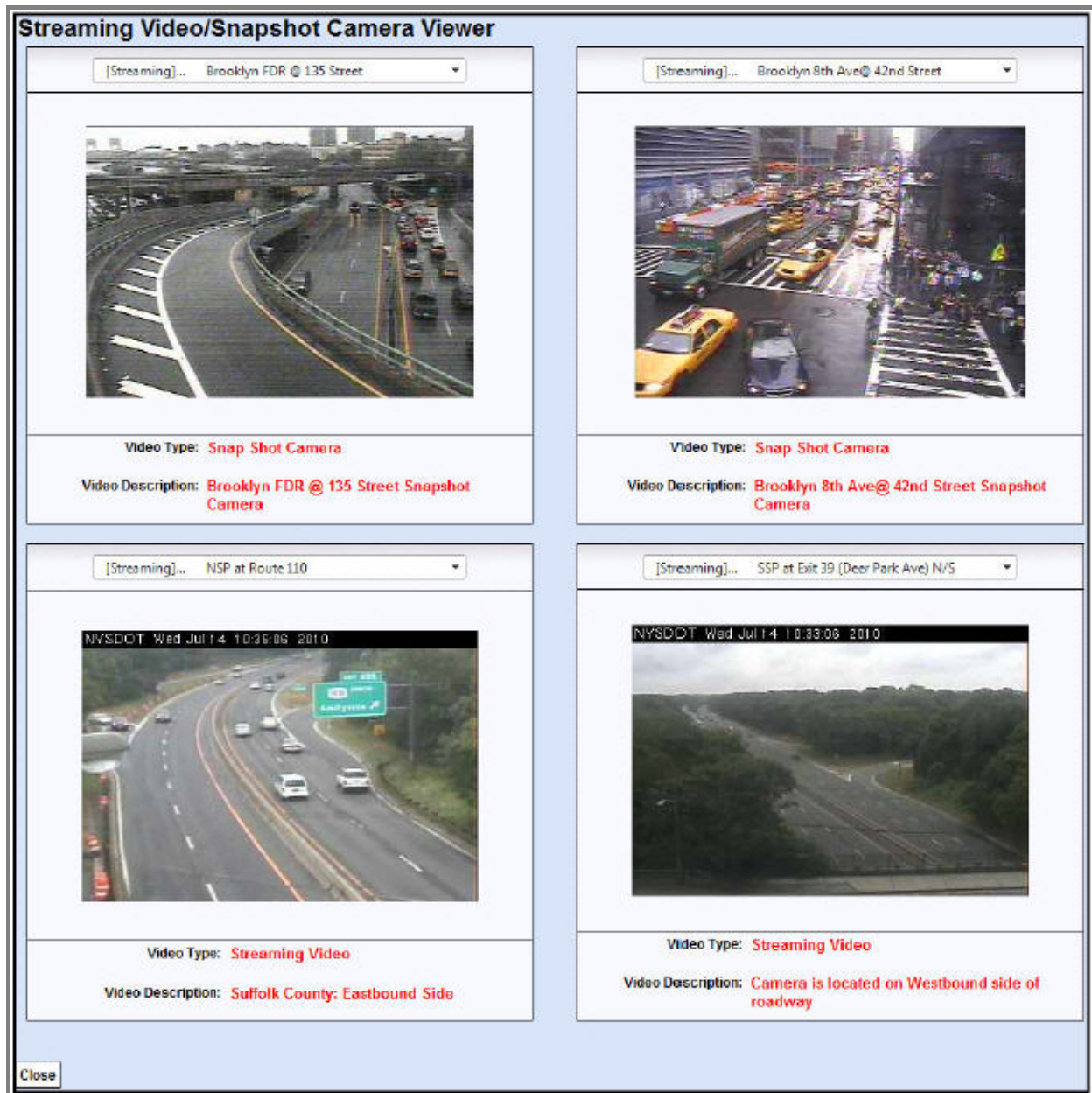


Figure 8: Streaming Video

System Setup and Access

- The Planning Module allows users to enter information about people and organizations, stockpile tracking, the ability to tie resources to an organization, and resource matching with Call Center tickets.
- DisasterLAN has the capabilities to track personal, contact, organization associations, skills, training and demographic information for people entered into the system.

- DisasterLAN has the capability to organize, inventory, and locate NIMS and non-NIMS resources. **Figure 9: Resource Typing** illustrates the differences between the descriptions of these resources.

The screenshot shows the 'Resource Information' window with the 'Descriptions' tab selected. The 'Kind of Resource' dropdown is set to '4X4 Vehicle'. The description field contains the text '4 wheel drive vehicle'. The 'NIMS Resource Type' dropdown is set to '-- None Available --'. Buttons for 'Submit' and 'Cancel' are visible at the bottom right.

The Descriptions Panel

The screenshot shows the 'Resource Information' window with the 'Descriptions' tab selected. The 'Kind of Resource' dropdown is set to 'Air Ambulance (Fixed-Wing)'. The description field contains the text 'Air Ambulance (Fixed-Wing)'. The 'NIMS Resource Type' dropdown is set to '-- Select a NIMS Classification --'. A detailed table of capabilities and metrics is displayed below the description field.

Resource: Air Ambulance (Fixed-Wing)							
Category:		Health & Medical (ESF #6)			Kind:		Aircraft
Minimum Capabilities:							
Component	Metric	Type I	Type II	Type III	Type IV	Other	
Team	Care provided	Critical Care and Advanced Life Support	Critical Care and Advanced Life Support	Advanced Life Support	Basic Life Support		
Personnel	Minimum Staff	Same as Type II	Same as Type III	3 pilot 2 paramedics or 1 paramedic and 1 nurse or physician	2 pilot 1 paramedic		
Team	Transport	2 or more litter patients	1 litter patient	2 or more litter patients	1 litter patient		
Aircraft	Fixed-wing capabilities	Same as Type II	Same as Type III, plus IFR	Same as Type IV	Night operations		
Equipment		Same as Type II	Ability to deploy a	Same as Type IV	ALS ambulance		

The Descriptions Panel after Selecting a NIMS Resource

Figure 9: Resource Typing

- DisasterLAN comes preloaded with the standard ICS forms as shown in **Figure 10: Standard ICS Forms Menu**.

Version: 7.3.1
Demonstration

Incident: Buffalo Snow Storm
Your current role is: BCG Support Staff (IT)

Fri May 21, 2010 11:24:08
You are logged in as: demonstrationuser2. [Logout]

ICS Forms

Groups: Buffalo Computer Graphics Support

Name ▲	Description
ICS 201	Incident Briefing
ICS 202	Incident Objectives
ICS 203	Organization Assignment List
ICS 204	Division Assignment List
ICS 205	Incident Radio Communications Plan
ICS 206	Medical Plan
ICS 207	Organization Chart
ICS 209	Incident Status Summary
ICS 210	Status Change Card
ICS 211	Incident Check-in List
ICS 213	General Message
ICS 214	Unit Log
ICS 215	Operational Planning Work Sheet
ICS 215a	Incident Action Plan Safety Analysis
ICS 216	Radio Requirements Worksheet
ICS 217	Radio Frequency Assignment Worksheet
ICS 218	Support Vehicle Inventory
ICS 219-2	Card Stock - Green (Crew)
ICS 219-4	Card Stock - Blue (Helicopter)
ICS 219-6	Card Stock - Orange (Aircraft)
ICS 219-7	Card Stock - Yellow (Dozers)
ICS 220	Air Operations Summary
ICS 221	Demobilization Checkout
ICS 224	Crew Performance Rating
ICS 225	Incident Personnel Performance Rating
ICS 226	Individual Performance Ratings
ICS 308A	Resource Order Form A
ICS 308B	Resource Order Form B

Main Menu Back

Figure 10: Standard ICS Forms Menu

Other Items

- DisasterLAN provides a method of selecting only the calls that have been routed to a specific person. For example, all of the calls for the Incident Commander for a specific incident are shown in **Figure 11: Call Center Call List**.

DISASTER		Version: 7.4 Demonstration	Incident: Buffalo Snow Storm				Tue Jul 13, 2010 10:35:48				
			Your current role is: BCG Support Staff (IT)				You are logged in as: demonstrationuser. (Logout)				
Summary of: All Request, All Offers, All Reports Routings: _Incident Commander Incidents: Buffalo Snow Storm Priority: All Status: Approved, Assigned/Awaiting Demob, New Call, Reviewed, Tasked Sort: TimeModified DESC Total Calls: 9											
Routings: <input type="text" value="_Incident Commander"/> <input type="button" value="Routings"/> Start Date: <input type="text"/> End Date: <input type="text"/> Text: <input type="text"/> <input type="button" value="Reset"/> Search From: <input type="text"/> To: <input type="text"/> For: <input type="text"/> <input type="button" value="Go"/>											
<input type="checkbox"/>	Call #	<input type="checkbox"/>	Priority	Call Type	Call Kind	Status	Routed To	Time Modified	Specifics	Action	
<input checked="" type="checkbox"/>	2553	<input type="checkbox"/>	Extreme	Request	Generators - (Type II)	New Call	_Incident Commander	7/13/2010 10:35:26	test	Print Open	
<input checked="" type="checkbox"/>	2502	<input type="checkbox"/>	Extreme	Request	Generators - (Type II)	New Call	_Incident Commander, _Logistics Section (LOG), _Logistics Section Chief, _Logistics Section Deput...	7/13/2010 10:33:31	Power outage; generator needed as soon as possible.	Print Open	
<input type="checkbox"/>	2503	<input type="checkbox"/>	Extreme	Donation/Offer	Generators - (Type II)	Approved	_Incident Commander, _Logistics Section (LOG), _Logistics Section Chief, _Logistics Section Deput...	7/13/2010 10:32:27	1 Type II Generator available acquiring the asset from orange county. will be available in an hour	Print Open	
<input checked="" type="checkbox"/>	2504	<input type="checkbox"/>	High	Report	Power Outage	Tasked	_Incident Commander, _Logistics Section (LOG), _Logistics Section Chief, _Logistics Section Deput...	7/13/2010 10:29:56	Power out to entire block of houses.	Print Open	
<input type="checkbox"/>	2447	<input type="checkbox"/>	High	Report	Explosion	New Call	_Incident Commander, _Logistics Section (LOG), _Logistics Section Chief	9/28/2009 15:31:39	A house was blown up No one was injured...	Print Open	
<input type="checkbox"/>	2501	<input type="checkbox"/>	Low	Donation/Offer	4X4 Vehicle	New Call	_Logistics Section (LOG), _Logistics Section Chief, _Logistics Section Deputy, _Incident Commande...	9/25/2009 14:00:34	One 6 passenger vehicle available.	Print Open	
<input type="checkbox"/>	2500	<input type="checkbox"/>	Low	Request	4X4 Vehicle	New Call	_Incident Commander, _Logistics Section (LOG), _Logistics Section Chief, _Logistics Section Deput...	9/25/2009 13:52:57	Needed as soon as possible but not an emergency situation.	Print Open	
<input type="checkbox"/>	2433	<input type="checkbox"/>	Medium	Report	Bridge Closing	New Call	_Incident Commander, Agency - DOT, Agency - Thruway, ESF 3 - Public Works and Engineering, ESF 1...	9/29/2008 13:33:52	The Peace Bridge has been closed temporarily due to ice build-up, high wind, and blowing snow creating dangerous driving conditions. The bridge is expected to re-open by 9am tuesday morning.	Print Open	
<input type="button" value="Add Call"/>		<input type="button" value="Print Tickets"/>		<input type="button" value="Print Table"/>		<input type="button" value="Statistics"/>		<input type="button" value="Search"/>		<input type="button" value="Report Generator"/>	<input type="button" value="Forward"/>
<input type="button" value="Main Menu"/>		<input type="button" value="Call Center Management Menu"/>				<input type="button" value="Back"/>					

Figure 11: Call Center Call List

4.0 Appendix A: National Incident Management System (NIMS) Criteria

The following information in this appendix was provided to assessors prior to and during the evaluation as identified in the National Incident Management System Supporting Technology Evaluation Program (NIMS STEP) Guide, September 2010.

4.1 Purpose

This appendix was developed to serve as a procedural aid to assessors reviewing a product. All assessors have a full understanding of the methodology that will be used in this process and the proper application of the selected criteria. This guide provides an overview of the methodology to be used in the process as well as step-by-step instructions for conducting the inspection. The appendix specifically identifies and further describes the criteria assessors are to use and provides them with instructions for completing the applicable NIMS STEP Worksheet. Assessors are required to provide narrative explanations and general observations for select questionnaire responses.

The scope of the evaluation will be determined during the product selection and planning phase. Products are evaluated for National Incident Management System (NIMS) concepts and principles and relevant NIMS recommended technical standards. If a product does not implement any of the technical standards, evaluators will review the product solely for NIMS concepts and principles utilizing the NIMS STEP Worksheet. Products that are primarily focused on implementing technical standards (such as alert and warning systems) will be evaluated utilizing the NIMS STEP Worksheet – Technically Focused Evaluations. This worksheet provides assessors an opportunity to comment on relevant NIMS concepts and principles but focuses on implementation considerations and provides a product overview.

4.2 Instructions

The results of the process will be a description of the relevance of the product to NIMS. This is accomplished by assessing how applicable each product is to criteria from NIMS, and addressing subjective questions related to each criterion and the product as a whole.

The process includes three steps:

- Step 1: Review the NIMS criteria.
- Step 2: Apply each NIMS criterion to, and answer the questions for, the product.
- Step 3: Address the general questions to the product as a whole.

4.3 Step 1 – Review the NIMS Criteria

NIMS criteria were developed by a cross-section of Subject Matter Experts (SME) and select members of the emergency response community. Assessors inspect the product’s incorporation of NIMS concepts and principles. The primary sub-elements of the NIMS portion of the evaluation are as follows:

- Emergency Support
- Hazards
- Preparedness
- Communications and Information Management
- Resource Management
- Command and Management
- Assessors also review general questions on the product including but not limited to implementation considerations.

Assessors conduct qualitative analysis and provide feedback for all of the criteria listed above. Input from the assessors is captured using a Dichotomous rating scale – a quantitative method for measuring the agreement or disagreement for a set of NIMS-related statements. These methods are designed to help describe products and to determine the presence or absence of desirable attributes. **Table 13: NIMS Criteria Rating Summary** is reflected below; assessors complete this table for inclusion in applicable evaluation reports. The numbers provided will summarize ratings for Minimum Product Requirements within each NIMS criterion.

Table 13: NIMS Criteria Rating Summary

NIMS Criteria (Number of Minimum Product Requirements)	# Agree	# Disagree	# Not Applicable
Emergency Support (1)			
Hazards (1)			
Preparedness (1)			
Communications and Information Management (9)			
Resource Management (10)			
Command and Management (2)			

Assessors have identified key elements within each of the NIMS criterion that are cited as Minimum Product Requirements (**Table 14: Minimum Product Requirements**). These requirements were derived from the NIMS document and their ratings in the NIMS STEP Worksheet impact the overall rating of the product’s adherence to NIMS concepts and principles.

Table 14: Minimum Product Requirements

Reference Number	Minimum Product Requirements Text	NIMS Criteria
1	The product is consistent with the applicable Emergency Support Functions (ESFs) and core functions of the Incident Command System (ICS).	Emergency Support
2	The product can be used to plan for, or respond to, at least one hazard.	Hazards
3	The product can be used to support one or more core preparedness activities: planning; procedures and protocols; or training and exercises.	Preparedness
4	If the product uses ICS forms, they remain consistent with the ICS form numbers and purpose of the specific type of form as identified by NIMS.	Communications and Information Management
5	The product is interoperable with other systems at the level of custom-interfaced applications, one-way standards-based sharing, or two-way standards-based sharing.	Communications and Information Management
6	The product can be used to respond to small scale incidents and events.	Communications and Information Management
7	The product can be used to respond to large scale incidents and events.	Communications and Information Management
8	The product can be used by a single jurisdiction during incidents and events.	Communications and Information Management
9	The product can be used across the full spectrum of multi-agency incidents and events.	Communications and Information Management
10	The product can be used across the full spectrum of multi-discipline incidents and events.	Communications and Information Management
11	The product adheres to the principle of plain language (clear text).	Communications and Information Management
12	The product provides controls to restrict access to sensitive information.	Communications and Information Management
13	The product addresses the use of Mutual Aid Agreements and resources.	Resource Management
14	The product provides an integrated means for resource typing definitions.	Resource Management
15	The product provides a means for inventorying Federal Emergency Management Agency (FEMA) typed resources.	Resource Management
16	The product provides a means for inventorying non-FEMA typed resources.	Resource Management
17	The product provides a record of credentialed and other personnel.	Resource Management
18	The product provides a means for performing personnel and equipment accountability.	Resource Management
19	The product provides a means for resource requesting/ordering.	Resource Management
20	The product provides a means for resource tracking/reporting.	Resource Management

Reference Number	Minimum Product Requirements Text	NIMS Criteria
21	The product provides a means for resource recovery and demobilization.	Resource Management
22	The product assists in the reimbursement process.	Resource Management
23	Overall, the product is consistent with the applicable 14 ICS management characteristics.	Command and Management
24	If the product references ICS, the organization charts and/or terminology are consistent with it.	Command and Management

Additional descriptions associated with each NIMS criterion are outlined below.

4.4 Emergency Support

The selected product should be applicable to ESF and/or ICS. This is not to infer that a product cannot apply to a single category. Instead, it is intended to underscore a preference for product applicability across the greatest number of categories.

ESFs are defined in the NRF as:

- ESF #1 - Transportation
- ESF #2 - Communications
- ESF #3 - Public Works and Engineering
- ESF #4 - Firefighting
- ESF #5 - Emergency Management
- ESF #6 - Mass Care, Emergency Assistance, Housing, and Human Services
- ESF #7 - Logistics Management and Resource Support
- ESF #8 - Public Health and Medical Services
- ESF #9 - Search and Rescue
- ESF #10 - Oil and Hazardous Materials Response
- ESF #11 - Agriculture and Natural Resources
- ESF #12 - Energy
- ESF #13 - Public Safety and Security
- ESF #14 - Long-Term Community Recovery
- ESF #15 - External Affairs

Incident Command functions are defined in the NIMS document as follows:

- Incident Command

-
- Operations
 - Planning
 - Logistics
 - Finance/Administration
 - Intelligence/Investigations
 - Public Information
 - Safety
 - Liaison

4.5 Hazards

Each product should mirror the all-hazards philosophy of NIMS to the greatest extent possible. Assessors review the product's applicability to the general categories of natural and human-caused hazards, as defined by NIMS. The specific types of hazards identified in this section are from National Fire Protection Association (NFPA) 1600: Standard on Disaster/Emergency Management and Business Continuity Programs. The standard should be referenced for specific examples and detailed definitions. Following is a summary list of hazards for reference in the inspection of each product:

Natural hazards:

- Geological (earthquake, tsunami, volcano, landslide, etc.)
- Meteorological (flood, tidal surge, drought, forest fire, snow, windstorm, extreme temperature, etc.)
- Biological (emerging diseases [pandemic disease, West Nile virus, smallpox], animal or insect infestation, etc.)

Human-caused events:

- Accidental (hazardous material spill or release, explosion/fire, transportation accident, building/structure collapse, air/water pollution, contamination, etc.)
- Intentional (terrorism [explosive, chemical, biological, radiological, nuclear, cyber], sabotage, civil disturbance, etc.)

Technological-caused events:

- Technological-caused incidents (central computer, mainframe, software, or application, ancillary support equipment, telecommunications, energy/power/utility, etc.)

4.6 Preparedness

Effective emergency management and incident response activities begin with a host of preparedness activities conducted on an ongoing basis, in advance of any potential incident. Preparedness involves an integrated combination of assessment; planning; procedures and protocols; training and exercises; personnel qualifications, licensure, and certification; equipment certification; and evaluation and revision. Preparedness is a foundational step in emergency management and incident response; therefore, the concepts and principles that form the basis for preparedness are an integration of the concepts and

principles of all NIMS components. Assessors will identify the product's capability to support preparedness activities.

4.7 Communications and Information Management

Emergency management and incident response activities rely upon communications and information systems that support the formation of a common operating picture to all command and coordination sites. NIMS describes the requirements necessary for a standardized framework for communications and emphasizes the need for a common operating picture. NIMS is based upon the concepts of interoperability¹², reliability, scalability, portability, and the resiliency and redundancy of communication and information systems. When inspecting this criterion, the following subcategories should be considered: common operating picture, interoperability, scalability, plain language, and information security. Assessors will respond to questions in each area.

In terms of interoperability, assessors will identify the applicable level(s) of Technology/Data Elements as defined in the Interoperability Continuum developed by the Department of Homeland Security (DHS) SAFECOM program. The elements on the continuum are: Swap Files, Common Applications, Custom-Interfaced Applications, One-Way Standards-Based Sharing, and Two-Way Standards-Based Sharing. Refer to the SAFECOM Interoperability Continuum for detailed definitions of each element. For the purposes of the evaluation, data interoperability components must be integrated into the system's design and the vendor must demonstrate capabilities to share information with a disparate product, as applicable.

As related to scalability, NIMS is scalable to any situation from small, local events to large-scale incidents, whether pre-planned, forewarned, or no-notice. This scalability is essential for NIMS to be applicable across the full spectrum of multiple agency, multiple jurisdiction, statewide, and national events.

4.8 Resource Management

When inspecting resource management applications, three subcategories should be considered: preparedness, incident response, and post-incident recovery and reimbursement.

The preparedness activities (resource typing, credentialing, and inventory) are conducted on a continual basis to help ensure that resources are ready to be mobilized when called to an incident. Resource management during an event/incident includes requirements identification, ordering and acquiring, mobilizing, and tracking and reporting. Post-event activities include recovery/demobilization and reimbursement.

¹² Interoperability is defined as the ability of systems, personnel, and equipment to provide and receive functionality, data, information and/or services to and from other systems, personnel, and equipment, between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together. Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real time, when needed, and when authorized (NIMS, December 2008).

4.9 Command and Management

The Command and Management component within NIMS is designed to enable effective and efficient incident management and coordination by providing flexible, standardized incident management structure. The structure is based on three key organizational constructs: ICS, Multiagency Coordination Systems, and Public Information. ICS is based on 14 proven management characteristics, each of which contributes to the strength and efficiency of the overall system (Reference the NIMS Document December 2008, Component IV – Command and Management, for additional information). Assessors will rate the product’s applicability to each of the 14 management characteristics of ICS.

4.10 Other Criteria – Implementation and Product Overview

It is important to understand the implementation factors including the time and training impacts on governmental entities. This is especially important for small and rural agencies, which may have limited resources. Since specific product costs are typically negotiated at the time of sale, vendors are not required to provide product costs during the evaluation. However, assessors will identify associated expenditures that may be incurred in addition to the procurement of this product.

4.11 Step 2 – Apply NIMS Criteria and Complete NIMS STEP Worksheet

The second step in this review is to gain familiarization with the product and to apply the NIMS criteria. The test analyst will arrange training on the product or provide assessors with information on self-paced training, if applicable. The assessors will also have time allocated for use of the system to become familiar with the product’s capabilities.

Two sample NIMS STEP Worksheets are provided below. The appropriate worksheet related to product capabilities will be identified during the product selection and planning phase. Assessors are to review the product based on their application of the NIMS criteria. These reviews should be made according to a subjective inspection based upon the individual assessor’s knowledge of NIMS and experience.

4.12 Step 3 – Address General Questions

The third and final step is to address general questions for the product. The questions focus on addressing potential issues that may arise during implementation. For each question, assessors provide a detailed answer focusing on the ESF that they represent.

4.13 NIMS STEP Worksheet

The vendor’s completed product self-assessment is provided to assessors as a reference in order to facilitate an understanding of the product’s designed capabilities. Assessors should review the product and provide ratings for all questions during the evaluation, even those identified as not applicable by the vendor during the self-assessment. Assessors are not limited by the vendor’s responses.

Assessors will use the following guidance to complete the NIMS STEP Worksheet:

- Agree: The product is consistent with and effectively supports the statement presented.

-
- Disagree: The product is designed or intended to address the statement but the product is inconsistent with and does not effectively support the statement presented.
 - Not Applicable: The product is not designed or intended to address the statement presented.

5.0 Appendix B: Target Capabilities List (TCL) Core Capabilities

The following information in this appendix was provided to assessors prior to and during the evaluation as identified in the National Incident Management System Supporting Technology Evaluation Program (NIMS STEP) Guide, September 2010.

Assessors will identify the applicable core capabilities as defined in the Target Capabilities List (TCL). The TCL describes the capabilities related to the four homeland security mission areas: Prevent, Protect, Respond, and Recover. It defines and provides the basis for assessing preparedness. It also establishes national guidance for preparing the Nation for major all-hazards events, such as those defined by the National Planning Scenarios.

The current version of the TCL (September 2007) identifies 37 capabilities that were developed with active participation of stakeholders representing all levels of government, Non-Governmental Organizations (NGOs), and the private sector. The TCL is a national-level generic model of operationally ready capabilities defining all-hazards preparedness. The capability needs of various jurisdictions vary based on risk factors and special characteristics.

Assessors will utilize the form depicted in **Table 15: Core Target Capabilities Form** to record a subjective “yes” or “no” scoring determination as to if the product supports each particular capability. Support should be broadly determined based on both direct and indirect product support of the capability.

Assessors should answer the question: “Does the product being evaluated directly or indirectly support a capability that provides a means to accomplish mission and achieve desired outcomes by performing critical tasks, under specified conditions, to target levels of performance?” The complete TCL document is provided as a reference in the Incident Management Test and Evaluation Laboratory (IMTEL). Assessors may refer to the document for additional specifications for each core target capability, if needed.

Table 15: Core Target Capabilities Form

Core Target Capability	Supported by Product
Common Capabilities: Planning	
Common Capabilities: Communications	
Common Capabilities: Community Preparedness and Participation	
Common Capabilities: Risk Management	
Common Capabilities: Intelligence and Information Sharing and Dissemination	
Prevent Mission Capabilities: Information Gathering and Recognition of Indicators and Warning	
Prevent Mission Capabilities: Intelligence Analysis and Production	
Prevent Mission Capabilities: Counter-Terror Investigation and Law Enforcement	
Prevent Mission Capabilities: Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Detection	
Protect Mission Capabilities: Critical Infrastructure Protection	
Protect Mission Capabilities: Food and Agriculture Safety and Defense	
Protect Mission Capabilities: Epidemiological Surveillance and Investigation	

Core Target Capability	Supported by Product
Protect Mission Capabilities: Laboratory Testing	
Respond Mission Capabilities: On-Site Incident Management	
Respond Mission Capabilities: EOC Management	
Respond Mission Capabilities: Critical Resource Logistics and Distribution	
Respond Mission Capabilities: Volunteer Management and Donations	
Respond Mission Capabilities: Responder Safety and Health	
Respond Mission Capabilities: Emergency Public Safety and Security	
Respond Mission Capabilities: Animal Disease Emergency Support	
Respond Mission Capabilities: Environmental Health	
Respond Mission Capabilities: Explosive Device Response Operations	
Respond Mission Capabilities: Fire Incident Response Support	
Respond Mission Capabilities: Weapons of Mass Destruction (WMD) and Hazardous Materials Response and Decontamination	
Respond Mission Capabilities: Citizen Evacuation and Shelter-in-Place	
Respond Mission Capabilities: Isolation and Quarantine	
Respond Mission Capabilities: Search and Rescue (Land-Based)	
Respond Mission Capabilities: Emergency Public Information and Warning	
Respond Mission Capabilities: Emergency Triage and Pre-Hospital Treatment	
Respond Mission Capabilities: Medical Surge	
Respond Mission Capabilities: Medical Supplies Management and Distribution	
Respond Mission Capabilities: Mass Prophylaxis	
Respond Mission Capabilities: Mass Care (Sheltering, Feeding and Related Services)	
Respond Mission Capabilities: Fatality Management	
Recover Mission Capabilities: Structural Damage Assessment	
Recover Mission Capabilities: Restoration of Lifelines	
Recover Mission Capabilities: Economic and Community Recovery	

6.0 Appendix C: References

1. American Association for Laboratory Accreditation (A2LA), <http://www.a2la.org/>.
2. Buffalo Computer Graphics, www.buffalocomputergraphics.com, accessed November 2010.
3. CAPI_1Schema.xsd, July 2007.
4. Common Alerting Protocol (CAP) Test Procedures, August 2010.
5. Disaster Management Interoperability Services, (DMIS), <http://www.fema.gov/about/programs/disastermanagement/index.shtm>.
6. Emergency Data Exchange Language-Distribution Element (EDXL-DE) Test Procedures, August 2010, Draft.
7. National Incident Management System (NIMS), December 2008, <http://www.fema.gov/emergency/nims/>.
8. National Response Framework (NRF), January 2008, <http://www.fema.gov/emergency/nrf/>.
9. National Fire Protection Association (NFPA) 1600: Standard on Disaster/Emergency Management and Business Continuity Programs, 2007, <http://www.nfpa.org/>.
10. NIMS Recommended Standard List, January 2009 http://www.fema.gov/pdf/emergency/nims/FY09_Recommend_Standards_List_121708.pdf.
11. National Incident Management System Supporting Technology Evaluation Program (NIMS STEP): DisasterLAN Evaluation Plan, October 2010.
12. NIMS STEP Guide, September 2010.
13. Organization for the Advancement of Structured Information Standards (OASIS) Standard CAP-v1.1, October 2005, <http://www.oasis-open.org/home/index.php>.
14. OASIS Standard EDXL-DE v1.0, May 2006, <http://www.oasis-open.org/home/index.php>.
15. SAFECOM Interoperability Continuum, accessed October 2009, http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf.
16. Target Capabilities List (TCL), September 2007, <http://www.fema.gov/pdf/government/training/tcl.pdf>.
17. XRay™ 2 Extensible Markup Language (XML) Editor, <http://www.architag.com/xray/>.

7.0 Appendix D: List of Acronyms and Abbreviations

A2LA	American Association for Laboratory Accreditation
ALOHA	Area Locations of Hazardous Atmospheres
CAP	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
COG	Collaborative Operating Group
DCS	Data Collection System
DHS	Department of Homeland Security
DMIS	Disaster Management Interoperability Services
EDXL-DE	Emergency Data Exchange Language-Distribution Element
EDXL-RM	Emergency Data Exchange Language-Resource Messaging
EOC	Emergency Operations Center
ESF	Emergency Support Function
EST	Eastern Standard Time
FEMA	Federal Emergency Management Agency
GIS	Geographic Information Systems
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IEC	International Electrotechnical Commission
IMTEL	Incident Management Test and Evaluation Laboratory
ISO	International Organization for Standardization
IT	Information Technology
JFO	Joint Field Office

NFPA	National Fire Protection Association
NGO	Non-Governmental Organizations
NGSC	NIMS General Support Contract
NIC	National Integration Center
NIMS	National Incident Management System
NIMS STEP	National Incident Management System Supporting Technology Evaluation Program
NPD	National Preparedness Directorate
NRF	National Response Framework
OASIS	Organization for the Advancement of Structured Information Standards
OPEN	Open Platform for Emergency Networks
QC	Quality Control
SAIC	Science Applications International Corporation
SME	Subject Matter Expert
STT	STEP Test Tool
T&E	Test and Evaluation
TCL	Target Capabilities List
UC	Unified Command
WMD	Weapons of Mass Destruction
XML	Extensible Markup Language