National Incident Management System (NIMS) Supporting Technology Evaluation Program (STEP) Guide

July 2008

FEMA

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Cover Photo: Clanton, Alabama, 29 August 2005 - The FEMA Emergency Response Team (in balcony) work at the Alabama Emergency Operations Center. FEMA is monitoring Hurricane Katrina as it makes landfall on the gulf coast. FEMA/Mark Wolfe.

INTRODUCTION

This document is a comprehensive guide to the National Incident Management System Supporting Technology Evaluation Program (NIMS STEP). Evaluation activities are sponsored by the National Preparedness Directorate (NPD), Federal Emergency Management Agency (FEMA). This guide is designed to provide an orientation to the evaluation process and policies including vendor application materials, product selection methods, on-site evaluation activities, and post-evaluation review/reporting processes.

> ***"Systems operating in an incident management environment must be able to work together (across disciplines and jurisdictions) and not interfere with another. Interoperability and compatibility are achieved through the use of tools such as common communications and data standards, digital data formats, equipment standards, and design standards."***
>
> ***~ National Incident Management System***

Background

Homeland Security Presidential Directive (HSPD)-5 directed the Secretary of Homeland Security to develop and administer the National Incident Management System (NIMS). In 2004, the Department of Homeland Security (DHS) released NIMS to provide a consistent nationwide template to enable governments and responders to work together effectively and efficiently to manage incidents and planned events. Although the incident management framework can be adaptable to any situation, NIMS provides a standard structure and management concepts that transcend all incidents, including:

- Accountability
- Common Terminology
- Comprehensive Resource Management
- Information and Intelligence Management
- Integrated Communications
- Management Span-of-Control
- Modular Organization
- Unified Command Structure

The 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 work together and not interfere with one another. Interoperability and compatibility are achieved through the use of tools such as common communications and data standards. The NIMS STEP supports NIMS implementation by providing

> ***"NIMS defines standardized mechanisms and establishes the resource management process to: identify requirements, order and acquire, mobilize, track and report, recover and demobilize, reimburse, and inventory resources."***
>
> ***~ National Incident Management System***

an independent, third party evaluation of supporting technologies – the use and incorporation of new and existing technologies to improve efficiency and effectiveness in all aspects of incident management. The Incident Management Systems Integration (IMSI) Division of NPD has tasked the NIMS Support Center (NIMS SC) to support and manage the day-to-day functions of the program. The NIMS SC and the testing facility are located in Somerset, Kentucky. For additional information on the NIMS SC, refer to **Appendix B**.

Program Description

The purpose of NIMS STEP is to provide an independent, objective evaluation of commercial and government software and hardware[1] products to assist in the implementation of the NIMS. Evaluation activities are designed to expand technology solutions and provide the emergency response community with an objective process to evaluate their purchases. Vendor participation in NIMS STEP is voluntary and the evaluation results and use of trade names in the report do not constitute a DHS or FEMA certification or endorsement of the use of such commercial hardware or software. The evaluations do not constitute a determination of NIMS compliance.

> ***"Emergency management and incident response activities rely upon communications and information systems that provide 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 interoperability, reliability, scalability, portability, and the resiliency and redundancy of communication and information systems."***
>
> ***~ National Incident Management System***

NIMS STEP has been designed to evaluate incident management-related software and hardware against NIMS criteria and NIMS technical standards. The NIMS criteria assessment is conducted by Subject Matter Experts (SMEs) and is qualitative in nature. SMEs use criteria derived from the NIMS document (Publication FEMA 501). See **Appendix D** for a description of the assessment criteria. All vendor products in NIMS STEP will be evaluated against NIMS criteria.

NIMS technical standard evaluations are objective in nature and based upon adopted standards. NIMS STEP personnel evaluate vendor product's adherence to the Common Alerting Protocol (CAP) and the Emergency Data eXchange Language (EDXL) suite of standards. If a product does not implement either the CAP or Emergency Data eXchange Language Distribution Element (EDXL-DE) standards, evaluators will review the product solely for NIMS concepts

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

and principles. Additional standards may be included in the program as they are approved by IMSI.

The NIMS STEP has been designed to evaluate products that support emergency managers and responders in decision-making prior to and during an incident, such as the following types of products: (1) vulnerability analysis, hazard forecasting, and consequence assessment; (2) intellegence and analysis; (3) physical and cyber security, access control, and surveillance; (4) collaboration; (5) incident management; and (6) communication and network infrastructure.

Program Scope

NIMS STEP personnel evaluate products primarily in a controlled, simulated, Emergency Operations Center (EOC)-based environment. Some products require demonstration in a limited field setting. In these cases, the field setting is considered an extension of the laboratory environment. Evaluations take place typically over the course of one week during which recognized experts in the field of emergency management and response gain hands-on experience with the system. The team consists of objective evaluators, typically including one test engineer and at least three SMEs for each product under evaluation. Engineers conduct technical analysis of a product's adherence to the standards under review. The SMEs conduct qualitative analysis and provide feedback on the product based on concepts and principles from NIMS (Publication FEMA 501). Input from the SMEs is captured using a Dichotomous rating scale – a 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.

Benefits to Vendors

NIMS STEP supports vendors in their implementation of NIMS and associated standards, concepts, and principles. Vendors will receive a copy of the evaluation report including feedback from end-user representatives and test engineers; these services are provided at no cost to the vendor. Vendors may use results of the evaluation to demonstrate with users their commitment to NIMS and the use of standards to maintain interoperability with other applications or platforms. The results of the test may also support the vendor in identifying areas for enhancement during future development of their product. The report will also identify the capabilities of the system as related to its incorporation of NIMS concepts and principles as well as the product's adherance to the CAP and EDXL suite of standards, if applicable. The results from each evaluation will be posted on the Responder Knowledge Base (RKB) (https://www.rkb.us/) and System Assessment and Validation for Emergency Responders (SAVER) (https://saver.fema.gov) websites. These sites provide government officials and other end users with access to evaluated products and results.

Benefits to Emergency Management/Response Personnel

NIMS STEP supports practitioners in their decision making during the purchasing and procurement process. The primary benefits to Emergency Management/Response Personnel[2] include access to reports based on results from an objective evaluation. Practitioners can also utilize NIMS technical standards and criteria for reference when purchasing hardware and software off the shelf or in Requests For Proposals (RFPs) when developing new products.

EVALUATION PROCESS

Figure 1 provides an overview of the evaluation process. The following sections describe the application process, coordination between the NIMS STEP team and vendors, evaluation conduct, and the reporting process in more detail.

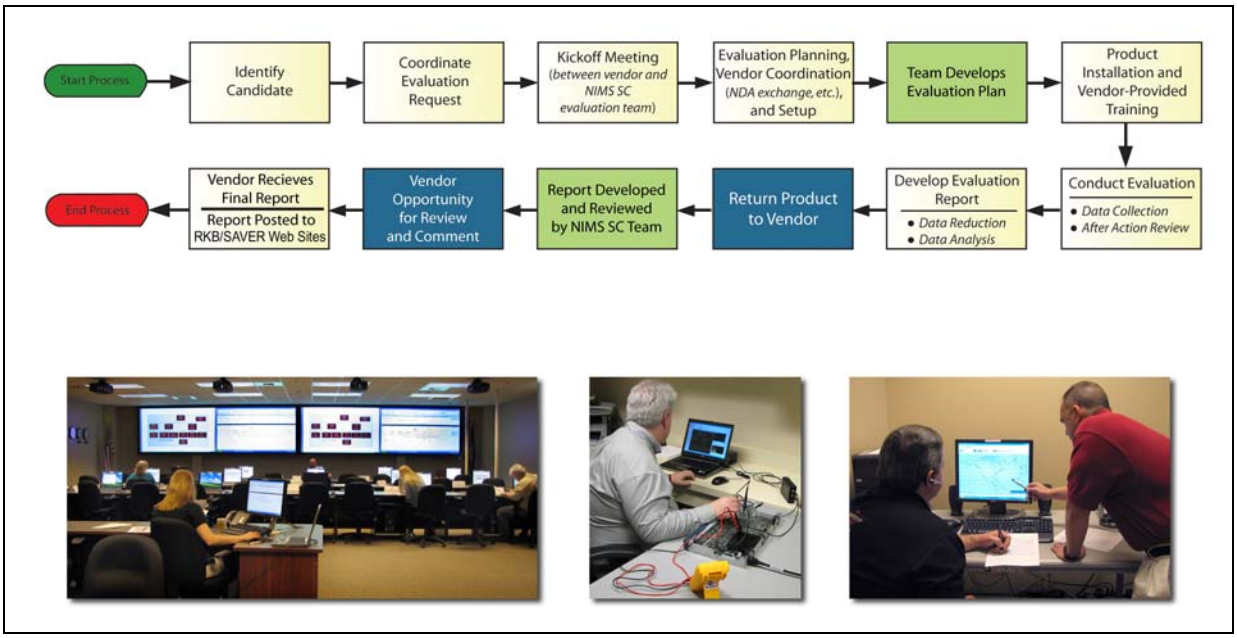

Figure 1: Evaluation Process Overview

[2] ***Emergency Management/Response Personnel:*** *Includes federal, state, territorial, tribal, substate regional, and local governments, private sector organizations, critical infrastructure owners and operators, Non-Governmental Organizations (NGOs), and all other organizations and individuals who assume an emergency management role. Also known as Emergency Responder. – National Incident Management System*

Application Materials

Vendors are responsible for completing all application materials and submitting documentation to the NIMS STEP team. The vendor application materials are available on the program website (http://www.nimsstep.org) and vendors should submit their application for evaluation using the online system. The forms in **Appendix A** provide examples of the questions provided online. The initial application should include *Vendor Application Part 1 – Intent for Evaluation* and supporting system documentation, as the vendor deems appropriate.

Product Selection

The program has established an objective process to select products for evaluation. Staff will review vendor applications based on the order they are received. Products will be reviewed for applicability to the program objectives and relevance to the emergency response and management community. Six major technology groups will be considered for evaluation.

1. **Vulnerability Analysis, Hazard Forecasting, and Consequence Assessment**: Software that provides emergency management/response officials with information on natural and infrastructure risks, forecasts incident consequences, and/or analyzes the impact of hazards based on demographic data and human needs. These products lead to decisions and response activities and increase confidence among officials and the public.

2. **Intelligence and Analysis**: Products that support multi-source collection and the production and dissemination of intelligence to incident response organizations so they can monitor threats, detect and prevent attacks, and alert authorities.

3. **Physical and Cyber Security, Access Control, and Surveillance**: Products that support site monitoring, personnel identification and authentication, and the detection of physical and electronic incursions that are fully integrated and interoperable with responder systems and analytical decision-support tools.

4. "**Back Office" Collaboration**: Collaboration software that facilitates strategic planning, emergency planning, multi-agency training and exercises, and shared decision-making.

5. **Incident Management**: Effective and efficient response requires command, control, and communication from tactical on-scene locations to local and state EOCs, as well as Federal operations centers. The real-time delivery of critical information among responders, emergency management officials, and executives at all levels of government is critical. Among other products that support these goals, resource management applications assist organizations inventory, track and report, request and order, and recover resources.

6. **Communication and Network Infrastructure**: Communication between interconnected wired and wireless networks and commercial systems for voice, text, graphic, video, and spatial information, providing broad-based intelligence and highly-focused operational information.

In order to be considered for an evaluation, products must meet minimum requirements as identified in the Vendor Application. Specifically, priority will be given to products that have the potential to meet a need in the field based on a written request from an emergency manager or responder, implement one or both of the recommended standards (CAP or EDXL-DE), have applicability to NIMS, and are mature enough in their development for evaluation. In applying for the program, vendors should consider both their timetable for future product releases and the maturity of their product. Products should be deployed in the field and not in a development or prototype phase to be considered for the program. The NIMS STEP staff will review application materials, and schedule evaluations based on the availability of program resources. The evaluation team will notify the applicant of the status of their application and proceed with evaluation planning to include an initial call from a member of the staff and coordination of a Non-Disclosure Agreement (NDA).

Evaluation Planning and Setup

Once a product is selected for evaluation, a member of the NIMS STEP staff will contact the vendor to introduce them to the evaluation process, to answer any questions they may have about the program, and to initiate logistics coordination activities. The evaluation team will coordinate a follow-on meeting with the vendor, during which the vendor can conduct a demonstration of their product. During the initial planning phase, evaluation staff will discuss requirements for a NDA and vendors will be asked to sign a *Vendor Consent Form* (**see Appendix A**) to indicate that they have read and agree to the policies outlined in this guide. Also, the program has an approved NDA process in place that will be coordinated with each vendor.

At the conclusion of the demonstration, vendors will be encouraged to complete supplementary vendor application materials within one week, specifically *Vendor Application Part 2 – Product Information Request Form, Part 3a CAP v1.1 Supplementary Mapping* (if applicable) and/or *Part 3b EDXL-DE v1.0 Supplementary Mapping* (if applicable). Supplementary application materials are included in **Appendix A**. Upon receipt of supplementary application materials, staff will develop a timeline for conducting the evaluation and coordinate detailed logistics with the vendor to include product installation/web access, supporting software/hardware requirements, evaluator training, and technical support for installation and evaluation conduct.

In the event that significant technical or operational issues surface prior to the evaluation, the team will advise the vendor. The vendor will then have the option to perform corrective actions, begin the evaluation without taking corrective actions, or withdraw from the evaluation. The evaluation begins at the start of product installation/setup after which the vendor will not be permitted to withdraw their product from the evaluation process.

Evaluation Conduct – NIMS Concepts and Principles

SMEs evaluate the product's incorporation of NIMS concepts and principles. The primary sub-elements of the NIMS portion of the evaluation are: Emergency Support, Scalability, Hazards, Resource Management, Communication and Information Management, and Command and Management. SMEs also review general questions on the product including Implementation Considerations. All evaluators receive training on the product and review available system documentation and training materials. At the conclusion of training, SMEs will work with the system during practical exercises and realistic scenarios to become familiar with system capabilities. After utilization of the system, SMEs will complete a *NIMS STEP Worksheet* and document their observations (**see Appendix D**). SMEs will evaluate products against established criteria to ensure they are consistent with NIMS concepts and principles. Certain criteria may not be applicable to all types of products and will be rated as Not Applicable (N/A). SMEs also provide qualitative responses along with their ratings. **Table 1** provides a notional summary of key findings for NIMS elements.

Table 1: NIMS Elements Summary Table (Notional)

NIMS Elements	Consistent with NIMS?		
	Agree	Disagree	N/A
1. Emergency Support	☒	☐	☐
2. Scalability	☒	☐	☐
3. Hazards	☒	☐	☐
4. Resource Management	☐	☐	☒
5. Communications and Information Management	☐	☒	☐
6. Command and Management	☒	☐	☐

Evaluation Conduct – Adherence to Standards

This second portion of the evaluation addresses the implementation of standards. In Fiscal Year (FY) 08, the program has the capability to test the adherence of products to the following two NIMS standards: CAP v1.1 and EDXL-DE v1.0. Additional NIMS standards may be incorporated in the NIMS STEP in FY09. Applicable standards will be referenced on the website

and in program documentation. The following sections provide a summary of each standard currently implemented in the evaluation program.

Common Alerting Protocol

The CAP is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent alert or warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings, which may help officials identify hazards and initiate the appropriate response. The evaluation cases for CAP are included in Table 2. The first three cases are specifically related to the CAP standard. The fourth evaluation case is derived based on the intent of the CAP standard to facilitate interoperability and information sharing. For the purposes of the transaction evaluation case (EVAL_004), a disparate system is defined as a third party application or product (government or commercial). To successfully demonstrate transaction, the system under evaluation must send/receive CAP messages (as applicable to the product) to a minimum of one disparate system. Evaluators provide a separate rating for sending and receiving. For additional information on the CAP standard refer to the Organization for the Advancement of Structured Information Standards (OASIS) website (http://www.oasis-open.org/home/index.php).

Table 2: CAP Evaluation Cases

Evaluation Case Identifier	Evaluation Case Title	Evaluation Objective
EVAL_001	Generate CAP Alert Message	Generate a CAP Alert message for use in the eXtensible Markup Language (XML)/Schema validation, CAP conformance, and transaction testing.
EVAL_002	XML/Schema Validation	Determine if the message is well formed and valid against a CAP 1.1 applied schema.
EVAL_003	CAP Conformance	Determine if the CAP standard is applied in the correct format to include proper application of cardinality of elements, CAP standard structure, mandatory and optional elements, and conditional rules.
EVAL_004	Transaction	Verify transaction (send and / or receive) with disparate systems.

Notional results of adherance to specific standards may be reported in a summary format similar to that depicted in **Table 3** for CAP. Products are not assigned a pass/fail rating; they are judged on a scale as depicted below. The items shown in bold negatively impacted the rating in that area. The other items provided are observations.

Table 3: CAP Evaluation Results (Notional)

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 (N/A) to the system.

Evaluation Case Identifier	Evaluation Case Title	Rating	Key Findings
EVAL_001	Generate CAP Alert Message		This system can be used to develop CAP alert messages. Engineers successfully entered all required and optional elements. System provides a direct method to save and extract the CAP XML file.
EVAL_002	XML/Schema Validation		Minor issues were identified with the format of the CAP alert message content. Messages were well formed but **did not validate against the CAP 1.1 schema due to an incorrect date/time format.**
EVAL_003	CAP Conformance		Minor issues were identified with the conformance to the CAP standard. **The system did not use a proper date/time format for the "sent" element. Additionally, the "identifier" element included spaces.** Engineers confirmed the presence of all mandatory elements and proper cardinality of all elements. All business rules were properly implemented. Does not include optional elements include "Digest" and "Parameter".
EVAL_004	Transaction (send)		Engineers sent CAP alert messages from the system under test to Disaster Management Interoperability Services (DMIS) using Open Platform for Emergency Networks (OPEN). **Due to the discrepancy with the date/time format, three optional elements (<effective>, <onset>, and <expires>) did not display properly when received by DMIS.**
	Transaction (receive)		**This system rejected incoming messages from DMIS. This problem was attributed to issues with the <derefUri> element.**

Emergency Data eXchange Language-Distribution Element

The Distribution Element specification describes a standard message distribution framework for data sharing among emergency information systems using the XML-based EDXL. This format may be used over any data transmission system, including the Simple Object Access Protocol (SOAP) Hypertext Transfer Protocol (HTTP) binding. For additional information on the EDXL-DE standard refer to OASIS website (http://www.oasis-open.org/home/index.php). The EDXL-DE evaluation cases are structured in a format similar to the CAP cases. The test cases for EDXL-DE are included in **Table 4**.

Table 4: EDXL-DE Evaluation Cases

Evaluation Case Identifier	Evaluation Case Title	Evaluation Objective
EVAL_EDXL-DE_001	Generate EDXL-DE Alert Message	Generate an EDXL-DE message for use in the EDXL-DE XML/Schema validation, conformance, and transaction testing.
EVAL_EDXL-DE_002	XML/Schema Validation	Determine if the message is well formed and valid against an EDXL-DE 1.0 applied schema.
EVAL_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.
EVAL_EDXL-DE_004	Transaction	Verify transaction (send and / or receive) with disparate systems.

Notional results of adherance to specific standards may be reported in a summary format similar to that depicted in **Table 5** for EDXL-DE. Products are not assigned a pass/fail rating; they are judged on a scale as depicted below. The items shown in bold negatively impacted the rating in that area. The other items provided are observations.

Table 5: EDXL-DE Evaluation Results (Notional)

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 (N/A) to the system.

Evaluation Case Identifier	Evaluation Case Title	Rating	Key Findings
EVAL_EDXL-DE_001	Generate EDXL-DE Alert Message		EDXL-DE messages were automatically generated based on modification of incident information.
EVAL_EDXL-DE_002	XML/Schema Validation		EDXL-DE messages properly validated to the schema.
EVAL_EDXL-DE_003	EDXL-DE Conformance		Messages properly conformed to the EDXL-DE standard.
EVAL_EDXL-DE_004	Transaction (send)		EDXL-DE messages were successfully sent to OPEN and a disparate system**. One optional element <senderRole> permitted multiple entries but the system only sent the first entry.**
	Transaction (receive)		The product's primary purpose is to generate and send messages. It does not provide the capability to receive messages.

Data Collection, Analysis, and Reporting

The primary data collected during evaluations is one collective NIMS STEP Worksheet, a set of completed evaluation procedure logs for the CAP evaluation, and one for the EDXL-DE evaluation (as applicable to the product). All participants submit observations electronically through the Test and Evaluation (T&E) Data Collection System (DCS) and participate in after-

action reviews. Data analysis and Quality Control (QC) begin during the evaluation and conclude with the development of an evaluation report.

The evaluation team's report will include a description of events that occurred during the evaluation; results regarding NIMS elements and adherence to each of the identified standards; and references to product documentation. The report may also include participant observations and select comments/ratings from evaluation team members.

Vendors will have an opportunity to review a draft of the evaluation report within 30 working days after completion of the evaluation. The vendor may submit comments and a response for inclusion as an appendix to the report within 10 working days of receipt of the draft.

Follow-on Testing

The vendor has the option to request a re-test when providing a response to the draft report. Follow-on tests are typically limited to products which did not meet the standards in one or more areas and that provide documentation to demonstrate that corrective actions have been completed. Re-tests will be scheduled based on resource availability and evaluation schedules. The original evaluation report will be submitted to the websites and the results of the re-test will supplement original findings. An application form for a re-test is included in **Appendix A:** *Vendor Application Part 4 – Request for Re-test.* If major system upgrades are performed, vendors will have the opportunity to resubmit their product for evaluation through the standard application process.

Program Websites

The vendor application materials are available on the program website and vendors should submit their application for evaluation using the online system (http://www.nimsstep.org). The website will also address Frequently Asked Questions and include a copy of this Guide. The results from each evaluation will be posted on the RKB (https://www.rkb.us/) and SAVER (https://saver.fema.gov) websites regardless of the outcome. By participating in the program, vendors provide their consent to IMSI Division regarding the posting of the results for public viewing. The evaluation results and use of trade names on the program website do not constitute a DHS or FEMA certification or endorsement of the use of such commercial hardware or software. The evaluations do not constitute a determination of NIMS compliance.

Program Improvement

The evaluation program includes a process for soliciting and addressing feedback from vendors in order to ensure continuous program improvement. This will include a questionnaire for all vendors participating in the evaluation program. The Communications and Information Management Working Group and IMSI Division will review vendor comments and suggest changes to the program.

ROLES AND RESPONSIBILITIES

Table 6 outlines the roles and responsibilities of participating agencies.

Table 6: Participating Agencies

Organization	Roles and Responsibilities
National Preparedness Directorate	FEMA's NPD provides strategy, policy, and planning guidance to build prevention, protection, response, and recovery capabilities among all levels of government throughout the Nation. The IMSI Division of NPD oversees response policy by maintaining, revising, and disseminating the NIMS, the National Response Framework (NRF), and related materials. The IMSI Division directs and provides oversight of the NIMS STEP. They are also responsible for identifying standards for the NIMS STEP team to implement. Although removed from the evaluation itself, IMSI will make final decisions about all program process matters.
National Incident Management System Support Center	The IMSI Division of NPD has tasked the NIMS SC to support and manage the day-to-day functions of the NIMS STEP. The NIMS SC and the testing facility are located in Somerset, Kentucky. The evaluation team consists of a test director, analysts, SMEs, test engineers, data collectors, and Information Technology (IT) Personnel. Evaluators adhere to a NDA and a code of conduct which ensures objectivity and the protection of company sensitive information. SMEs conducting the evaluation of NIMS concepts and principles have extensive training and experience in emergency management and response and maintain updated knowledge regarding issues and practices in their discipline. Evaluators may be generalists or practitioners within the field of emergency management and response. All evaluators have a thorough understanding of emergency management principles and the concepts and principles of NIMS. Specifically, SMEs will be required to meet minimum qualifications in the following areas: years of experience in their discipline (e.g. medical, fire, law enforcement, etc.), completed courses (e.g. IS-100, IS-200, etc.), participation in responding to real-world incidents, and experience using software during exercises and/or real-world incidents. Test Engineers will be qualified in a technical field and will be required to have demonstrated experience in their domain (e.g. electrical engineering, software test, etc.).
NIMS Communications and Information Management Working Group	The Communications and Information Management Working Group will be composed of approximately 10 practitioners and SMEs familiar with information management standards and test and evaluation. The group will provide the IMSI Division and the NIMS STEP team with input regarding the application of NIMS standards in the program. For additional information on the working group including a summary of their roles and responsibilities refer to **Appendix C**.
Vendors	Vendors are responsible for completing application materials and, if selected, for training evaluators in a manner consistent with typical end-user training. Vendors will be required to provide evaluators with access to their system, and to provide technical support during system installation and product evaluation. Typically, vendors can provide all required support remotely.

APPENDIX A: APPLICATION MATERIALS

A vendor consent form will be coordinated with the vendor during the evaluation planning process. Vendor Application Forms 1 through 4 will be available through the program website. Vendors should apply using the forms available online (http://www.nimsstep.org). The following forms are provided solely for informational purposes.

Vendor Consent Form

In order to participate in the NIMS STEP, vendors must sign the following consent form. By participating in the program, vendors provide their consent to the IMSI Division regarding the posting of the results/report for public viewing. In the event that significant technical or operational issues surface prior to the evaluation, the team will advise the vendor. The vendor will then have the option to perform corrective actions, begin the evaluation without taking corrective actions, or withdraw from the evaluation. Once the evaluation begins, the vendor will not be permitted to withdraw.

By signing this form, I agree to the aforementioned terms and have read and agree to the policies outlined in this NIMS STEP Guide, dated July 2008.

Signature: _____
Name (printed): _____
Title: _____
Date: _____
Address: _____
_____
_____
Telephone No.: _____

Vendor Application Part 1 – Intent for Evaluation

This is the initial application form for vendors who express interest in participating in the NIMS STEP. Priority will be given to products that have the potential to meet a need in the field based on a written request from an emergency manager or responder, implement one or both of the recommended standards (CAP or EDXL-DE), have applicability to NIMS, and are mature enough in their development for evaluation.

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Address:	
City:	
State:	
Zip Code:	
E-mail:	
Phone Number:	
Alternate Phone Number:	
Fax Number:	

1. Product Name:	
2. Version Number:	
3. Product Description:	
4. If information is available online please provide Uniform Resource Locator(s) (URL):	
5. Indicate the product type:	☐ Vulnerability Analysis ☐ Hazard Forecasting ☐ Consequence Assessment ☐ Intelligence and Analysis ☐ Physical and Cyber Security ☐ Access Control ☐ Surveillance ☐ Collaboration ☐ Incident Management ☐ Communication and Network Infrastructure ☐ Other:
6. Describe the system configuration or architecture (e.g., accessible via the internet, installed on standalone client workstations, installed on a network, etc.):	

7. Please indicate who you anticipate will be the primary users of this hardware/software product:	
8. Does the product provide for a method for data sharing or interoperability? Identify any systems the product can share information with, or is interoperable with:	
9. Identify any standards used in the development of the product (e.g. CAP, EDXL-DE, etc.):	
10. Describe where the product is in the development lifecycle (e.g. prototype, pilot test phase, deployed, etc.):	
11. If the product is currently used in the field, provide examples of facilities, jurisdictions, counties, states, or other entities currently using the product: Note: Priority will be given to products that have the potential to meet a need in the field based on a written request from an emergency manager or responder. As a supplement to this form, please send any written requests to the NIMS STEP team at: NIMSSTEP@nimssc.net	

Vendor Application Part 2 – Product Information Request Form

This form is intended to assist staff in the detailed design and conduct of evaluation activities. It should be completed by a vendor representative through the online system upon notification that the product has been selected for evaluation; it is not required in the initial application package.

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Address:	
City:	
State:	
Zip Code:	
E-mail:	
Phone Number:	
Alternate Phone Number:	
Fax Number:	

1. Product Name:	
2. Version Number:	
3. Detailed Description (please provide a detailed description for the evaluation plan):	

4. Identify the supported operating system platform(s) (Windows, Unix, Linux, Macintosh, etc.):	
5. Identify product hardware support requirements (e.g. disk space, Random-Access Memory [RAM], processor, etc.):	
6. Identify product software support requirements (e.g. Oracle, Java, Structured Query Language [SQL] Server, MySQL, Access, Geographic Information Systems [GIS] software, etc.):	
7. Identify web requirements (e.g. browser, web server, etc.):	
8. Identify compliance with federal regulations (e.g. Americans with Disabilities Act [ADA], Health Insurance Portability and Accountability Act of 1996 [HIPAA], 508, etc.):	
9. Identify end-user training requirements (e.g. time required, type of training, etc.):	
10. Indicate who typically installs this product (vendor or end user). Describe installation process/requirements:	
11. Indicate availability of technical support from your organization during evaluation:	

12. Describe and provide a copy of all system documentation (user's guide, quick reference guide, training materials, etc.):	
13. Please provide any other general information that may assist the NIMS STEP team in the review of your product(s) (e.g. background info, etc.). Note that if the product incorporates the CAP or EDXL-DE standard the vendor will also need to complete Vendor Application Part 3a and/or 3b.	

Vendor Application Part 3a – CAP v1.1 Supplementary Mapping

This form is intended to assist staff in design and conduct of evaluation activities, specifically related to the evaluation of adherence to the OASIS CAP standard. It should be completed by a vendor representative through the online system upon notification that the product has been selected for evaluation; it is not required in the initial application package. Specify the origin of the contents of each CAP message element (e.g. user defined, auto-generated, or derived from other sources, etc.). Include the label used on the product's user interface and any algorithms or rules used to derive contents. For optional fields, also indicate the conditions under which this element appears or does not appear in the CAP message.

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Address:	
City:	
State:	
Zip Code:	
E-mail:	
Phone Number:	
Alternate Phone Number:	
Fax Number:	

Product Name:	
Version Number:	

Alert Element and Sub-elements

alert - Mandatory	**Origin, User Interface Label, Rules, Conditions, etc.**
Alert (alert) container <alert> … </alert>	N/A
Message ID (identifier):	
Sender ID (sender):	
Sent Date/Time (sent):	
Message Status (status):	
Message Type (msgType):	
Scope (scope):	

alert - Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
Source (source):	
Restriction (restriction):	
Addresses (addresses):	
Handling Code (code):	
Note (note):	
Reference IDs (references):	
Incident IDs (incidents):	

Info Element and Sub-elements (if used)

info – Mandatory	**Origin, User Interface Label, Rules, Conditions, etc.**
Info (info) container <info> … </info>	
Event Category (category):	
Event Type (event):	
Urgency (urgency):	
Severity (severity):	
Certainty (certainty):	

info - Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
Language (language):	
Response Type (responseType):	
Audience (audience):	
Event Code (eventCode):	
Effective Date/Time (effective):	
Onset Date/Time (onset):	
Expiration Date/Time (expiration):	
Sender Name (senderName):	
Headline (headline):	
Event Description (description):	
Instructions (instruction):	
Information URL (web):	
Contact Info (contact):	

Parameter (parameter):	

Resource Element and Sub-elements (if used)

resource - Mandatory	**Origin, User Interface Label, Rules, Conditions, etc.**
Resource (resource) container <resource> … </resource>	
Resource Description (resourceDesc):	

resource - Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
Multipurpose Internet Mail Extensions (MIME) Type (mimeType):	
File Size (size):	
Uniform Resource Identifier (URI) (uri):	
Dereferenced URI (derefUri):	
Digest (digest):	

Area Element and Sub-elements (if used)

area - Mandatory	**Origin, User Interface Label, Rules, Conditions, etc.**
Area (area) container <area> … </area>	
Area Description (AreaDesc):	

area - Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
Area Polygon (polygon):	
Area Circle (circle):	
Area Geocode (geocode):	

Altitude (altitude):	
Ceiling (ceiling):	

Please provide specific details and instructions on how to extract or obtain the CAP message once it has been generated (e.g. directly from a link in the software, any special software, servlet interface tool, etc.) for evaluation purposes. Please indicate if the CAP message generation is performed via manual CAP message entry, automatically, or uses both methods. Please also provide any additional requirements or specific restrictions of the product for CAP message generation outside of the OASIS CAP v1.1 standard.	

Vendor Application Part 3b – EDXL-DE v1.0 Supplementary Mapping

This form is intended to assist staff in design and conduct of evaluation activities specifically related to the evaluation of adherence to the OASIS EDXL-DE standard. It should be completed by a vendor representative through the online system upon notification that the product has been selected for evaluation; it is not required in the initial application package. Specify the origin of the contents of each EDXL-DE message element (e.g. user defined, auto-generated, or derived from other sources, etc.). Include the label used on the product's user interface and any algorithms or rules used to derive contents. For optional fields, also indicate the conditions under which this element appears or does not appear in the EDXL-DE message.

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Address:	
City:	
State:	
Zip Code:	
E-mail:	
Phone Number:	
Alternate Phone Number:	
Fax Number:	

Product Name:	
Version Number:	

EDXL Distribution Sub-elements

Required	**Origin, User Interface Label, Rules, Conditions, etc.**
EDXL Distribution – Top Level Container	N/A
distributionID:	
senderID:	
dateTimeSent:	
distributionStatus:	
distributionType:	
combinedConfidentiality:	

Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
language:	
senderRole:	
recipientRole:	
keyword:	
distributionReference:	
explicitAddress:	

Target Area Sub-elements (if used)

Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
targetArea – Container within EDXL Distribution	
circle:	
polygon:	
country:	

subdivision:	
locCodeUN:	

Content Object Sub-elements (if used)

Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
contentObject – Container within EDXL Distribution	
contentDescription:	
contentKeyword:	
incidentID:	
incidentDescription:	
originatorRole:	
consumerRole:	
confidentiality:	
other:	

Non-XML Content Sub-elements (if used)

Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
nonXMLContent – Container within Content Object	
mimeType: (required)	
size:	
digest:	
uri:	
contentData:	

OR

XML Content Sub-elements (if used)

Optional	**Origin, User Interface Label, Rules, Conditions, etc.**
xmlContent – Container within Content Object	
keyXMLContent:	
embeddedXMLContent:	

Please provide specific details and instructions on how to extract or obtain the EDXL-DE message once it has been generated (e.g. directly from a link in the software, any special software, servlet interface tool, etc.) for evaluation purposes. Please indicate if EDXL-DE message generation is performed via manual EDXL-DE message entry, automatically, or uses both methods. Please also provide any additional requirements or specific restrictions of the product for EDXL-DE message generation outside of the OASIS EDXL-DE v1.0 standard.	

Vendor Application Part 4 – Request for Re-Test

This form is intended to be completed by a vendor in the event that corrective action has been taken by that vendor on a significant issue identified during the initial test. It should be completed by a vendor representative through the online system.

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Address:	
City:	
State:	
Zip Code:	
E-mail:	
Phone Number:	
Alternate Phone Number:	
Fax Number:	

1. Product Name:	
2. Version Number:	
3. Description of Issue Identified during initial test:	
4. Description of corrective actions completed:	
5. Date product is available for re-test:	

APPENDIX B: FEDERAL PARTNERS AND THE NIMS SC

National Preparedness Directorate, FEMA

The 2006 Post-Katrina Emergency Management Reform Act mandated the creation of the NPD, unifying DHS' preparedness, mitigation, response, and recovery missions. Established on 1 April 2007, NPD oversees the coordination and development of the capabilities and tools necessary to prepare for terrorist incidents and natural disasters. The NPD provides strategy, policy, and planning guidance to build prevention, protection, response, and recovery capabilities among all levels of government throughout the Nation.

The National Integration Center (NIC), a division of the NPD, is responsible for developing, managing, and coordinating all homeland security training, education (external), exercise and lessons learned programs, as required, to ensure the Nation is prepared to prevent, protect against, respond to, recover from, and mitigate all hazards, natural or manmade. The Incident Management Systems Integration Division, situated within the NIC, oversees response policy by maintaining, revising, and disseminating the NIMS, the NRF, and related materials. IMSI oversees all aspects of NIMS including the development of compliance criteria and implementation activities at federal, state, and local levels. It provides guidance and support to jurisdictions and incident management and responder organizations as they adopt the system.

DHS Science and Technology Directorate

The NIMS STEP works closely with DHS's Test & Evaluation and Standards section. The Test & Evaluation and Standards section works across DHS and ensures that systems meet the capability needs of users, validates performance and provides measurable improvement to operational capabilities. Effective testing and evaluation programs provide crucial information to decision makers for acquisition and deployment of technology.

The NIMS STEP also collaborates with DHS's Command, Control and Interoperability Division. Their mission is to transform new and promising concepts into real operational capabilities. The Division is working with Federal partners to strengthen communications interoperability, improve Internet security and integrity, and accelerate the development of automated capabilities to help identify potential national threats.

NIMS Support Center

To support NIMS implementation, DHS established the NIMS SC in 2005 – a program that operates under a Cooperative Agreement between the FEMA and the Justice and Safety Center/Eastern Kentucky University (EKU). EKU has two strategic partners – Science Applications International Corporation (SAIC) and G&H International Services (GHIS) – that provide the NIMS SC with a variety of capabilities in support of NIMS implementation. The NIMS SC provides direct support to IMSI.

The NIMS SC is designed to develop new first responder tools, enhance technology integration, and evaluate and report on products and standards to improve incident

management and information sharing throughout the responder community. The program provides products and services in the following areas:

- Systems Development
- Standards and Test & Evaluation
- Technical Assistance and Incident Management Support

For additional information about the NIMS SC, please call or e-mail the staff at:

E-mail: FEMA-NIMS@dhs.gov
Phone: 202-646-3850

APPENDIX C: COMMUNICATIONS AND INFORMATION MANAGEMENT WORKING GROUP

Overview

The Communications and Information Management Working Group (Working Group) is formed to provide input into the NIMS STEP task area.

Composition

The Working Group represents a cross-section of stakeholders representing various emergency response disciplines, the test and evaluation community, as well as SMEs for the selected information sharing standards. Specifically, members are identified and selected based on their knowledge of and experience working with standards and test and evaluation. The composition of the Working Group generally reflects the following disciplines/areas of expertise:

- State NIMS Coordinator
- Emergency Management (Technical Representative)
- Fire (Technical Representative)
- Law Enforcement (Technical Representative)
- Public Health/ Emergency Medical Services/Hospital (Technical Representative)
- GIS/Mapping Specialist
- Vendor Representative
- Test and Evaluation Representative (Participant with former test and evaluation experience)
- Standard SME (Participant with expertise in a specific communication or information management field)
- Additional Public Safety Representative or Standard SME

Federal officials and NIMS SC staff may serve on the Working Group in an Ex Officio capacity. Specifically, test and evaluation officials from DHS' Science and Technology Directorate (most notably the Test and Evaluation and Standards Division and the Command, Control, and Interoperability Division) will be invited to participate on all Working Group activities.

Duties and Objectives

The objectives of the Working Group include the following:

- Review and provide input into process documentation (e.g., guidance materials, report templates, policy papers) for the NIMS STEP.
- Make recommendations on enhancements to all aspects of the NIMS STEP.
- Review feedback provided by vendors following the evaluation (e.g., post-evaluation questionnaires, informal "hotwash" comments).
- Review feedback provided to the NIMS SC from other sources.
- Make recommendations regarding the NIMS SC's NIMS STEP website, once developed.
- Make recommendations to the NIMS SC regarding hardware and software tools that would strengthen/support the test and evaluation process (i.e., simulation tools, communications devices and interfaces, etc.).
- Represent the emergency response community and areas of technical and operational expertise.

APPENDIX D: NIMS EVALUATION CRITERIA

Purpose

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

Evaluation Instructions

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

The process includes three steps:

- ***Step 1***: Review the Evaluation Criteria.
- ***Step 2***: Apply each Evaluation Criteria to, and answer the questions for, the product.
- ***Step 3***: Address the general questions to the product as a whole.

Step 1 – Review the Evaluation Criteria

The Evaluation Criteria was developed by a cross-section of SMEs and selected members of the emergency response community. Evaluators will be asked to evaluate the product against the following evaluation criteria:

- Emergency Support
- Scalability
- Hazards
- Resource Management
- Communication and Information Management
- Command and Management
- Implementation and Product Overview

SMEs conduct qualitative analysis and provide feedback for all of the criteria listed above. Input from the SMEs is captured using a Dichotomous scale – a quantitative method used to help measure positive or negative responses to NIMS-related statements. These methods are designed to help describe products and to determine the presence or absence of desirable attributes. A Summary Table is reflected below; evaluators will complete this table for inclusion in each evaluation report.

Table D-1: NIMS Elements Summary Table

NIMS Elements	Consistent with NIMS?		
	Agree	Disagree	N/A
1. Emergency Support	☐	☐	☐
2. Scalability	☐	☐	☐
3. Hazards	☐	☐	☐
4. Resource Management	☐	☐	☐
5. Communications and Information Management	☐	☐	☐
6. Command and Management	☐	☐	☐

Additional descriptions associated with each evaluation criterion are outlined below.

Emergency Support

The selected product should be applicable to Emergency Support Functions (ESF) and/or the Incident Command System (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:

- Transportation
- Communications
- Public Works and Engineering
- Firefighting
- Emergency Management
- Mass Care, Housing, and Human Services
- Public Health and Medical Services
- Resource Support
- Urban Search and Rescue
- Oil and Hazardous Materials Response
- Agriculture and Natural Resources
- Energy
- Public Safety and Security
- Long-Term Community Recovery and Mitigation
- External Affairs

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

- Incident Command
- Operations Function
- Planning Function
- Logistics Function
- Finance/Administration Function
- Intelligence Function
- Public Information Function
- Safety Function
- Liaison Function

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.

Hazards

Each product should mirror the all-hazards philosophy of NIMS to the greatest extent possible. Evaluators review the product's applicability to the general categories of natural and manmade hazards, as defined by NIMS. The specific types of hazards identified in this section are from the 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 evaluation 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.)

Manmade hazards:

Human-caused incidents

- 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 incidents

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

Resource Management

When evaluating 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. ***Communication 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 interoperability, reliability, scalability, portability, and the resiliency and redundancy of communication and information systems. When evaluating this criterion, four subcategories should be considered: plain language, incident reporting, interoperability, and security and vulnerability. SMEs will respond to questions in each area.

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: the Incident Command System, 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, Component IV – Command and Management, for additional information). SMEs will rate the product's applicability to each of the 14 management characteristics of ICS, as applicable.

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. The Ability to Readily Implement criterion is divided into two subcategories to consider time and training impacts associated with implementing the product. While specific product costs are typically negotiated at the time of sale, vendors are asked to provide an estimate of product costs during the evaluation.

Step 2 – Apply Evaluation Criteria and Complete Score Sheet

The second step in this review is to gain familiarization with the product and to apply the Evaluation Criteria. The Test Director will arrange training on the product or provide the

evaluator with information on self-paced training, if applicable. The evaluator will also have time allocated for use of the system to become familiar with the product's capabilities.

A sample NIMS STEP Worksheet is provided below. Evaluators are to review the product based on their application of the evaluation criteria. These reviews should be made according to a subjective evaluation based upon the individual evaluator's knowledge of NIMS and experience.

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, the evaluator must provide a detailed answer focusing on the ESF that they represent.

Table D-2: NIMS STEP Worksheet

Product Name:			
Evaluators:			
Criteria and Question	**Explanation**		
EMERGENCY SUPPORT *"EOCs may be organized by major discipline (e.g., fire, law enforcement, emergency medical services, etc.); by emergency support functions (e.g., transportation, communications, public works and engineering, resource support, etc.); by jurisdiction (e.g., city, county, region, etc.); or, more likely, by some combination thereof."* *– National Incident Management System* *"The Federal Government and many State governments organize much of their resources and capabilities – as well as those of certain private-sector and nongovernmental organizations – under 15 Emergency Support Functions (ESFs)."* *– National Response Framework*			
This product is applicable to _____ Emergency Support Functions.			
There are no obstacles to ESF(s) implementing this product.	Disagree ☐	Agree ☐	N/A ☐
Identify any obstacles to ESF(s) implementing this product.			
This product is applicable to _____ Incident Command functions.			
There are no obstacles to Incident Command functions implementing this product.	Disagree ☐	Agree ☐	N/A ☐
Identify any obstacles to Incident Command functions implementing this product.			
SCALABILITY *"Communications and information systems should be designed to be flexible, reliable, and scalable in order to function in any type of incident, regardless of cause, size, location, or complexity. They should be suitable for operations within a single jurisdiction or agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement." – National Incident Management System* *"It [the NRF] is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters." – National Response Framework*			
Identify any limitations on the system scalability.			

This product is applicable for use on small scale incidents and events.	Disagree	Agree	N/A
	☐	☐	☐
This product is applicable for use on large scale incidents and events.	Disagree	Agree	N/A
	☐	☐	☐
This product is applicable across the full spectrum of multi-agency incidents and events.	Disagree	Agree	N/A
	☐	☐	☐
This product is applicable across the full spectrum of multi-jurisdiction incidents and events.	Disagree	Agree	N/A
	☐	☐	☐
This product is applicable across the full spectrum of multi-discipline incidents and events.	Disagree	Agree	N/A
	☐	☐	☐
This product is applicable to multiple levels of government(s).	Disagree	Agree	N/A
	☐	☐	☐
List levels of government(s).			
This product is flexible enough to be applicable to the public and private sectors.	Disagree	Agree	N/A
	☐	☐	☐
If not, what are the limitations?			
HAZARDS *"Any incident, natural or manmade, that warrants action to protect life, property, environment, public health or safety, and minimize disruptions of government, social, or economic activities." – National Incident Management System* *"Communications and information systems should be designed to be flexible, reliable, and scalable in order to function in any type of incident, regardless of cause, size, location, or complexity." – National Incident Management System*			
This product is applicable to natural and manmade hazards.	Disagree	Agree	N/A
	☐	☐	☐
Identify applicable hazards.			

RESOURCE MANAGEMENT

"NIMS defines standardized mechanisms and establishes the resource management process to: identify requirements, order and acquire, mobilize, track and report, recover and demobilize, reimburse, and inventory resources."
– National Incident Management System

"A standardized, integrated process conducted prior to, during, and after an incident by all emergency management/response personnel and their associated organizations." – National Incident Management System

"The credentialing process is an objective evaluation and documentation of a person's current license or degree; training or experience; competence or certification; and the ability to meet nationally accepted minimum standards, to provide particular services and/or functions or perform particular procedures during an incident."
– National Incident Management System

This product addresses the need to manage resources.	Disagree	Agree	N/A
	☐	☐	☐
This product allows for the inventorying of resources.	Disagree	Agree	N/A
	☐	☐	☐
This product provides for the inventorying of FEMA typed resources.	Disagree	Agree	N/A
	☐	☐	☐
This product provides for the inventorying of non-FEMA typed resources.	Disagree	Agree	N/A
	☐	☐	☐
This product allows for personnel accounting.	Disagree	Agree	N/A
	☐	☐	☐
This product provides a record of credentialed personnel.	Disagree	Agree	N/A
	☐	☐	☐
This product provides a record of other personnel.	Disagree	Agree	N/A
	☐	☐	☐
This product provides for resource requesting/ordering.	Disagree	Agree	N/A
	☐	☐	☐
This product provides for resource tracking/reporting.	Disagree	Agree	N/A
	☐	☐	☐

This product provides for resource recovery.	Disagree	Agree	N/A
	☐	☐	☐
This product provides a reimbursement process.	Disagree	Agree	N/A
	☐	☐	☐
Identify any resource management comments.			
COMMUNICATION AND INFORMATION MANAGEMENT *"Codes should not be used, and all communications should be confined to essential messages. The use of acronyms should be avoided during incidents requiring the participation of multiple agencies or organizations."* *– National Incident Management System* *"Systems operating in an incident management environment must be able to work together (across disciplines and jurisdictions) and not interfere with one another. Interoperability and compatibility are achieved through the use of tools such as common communications and data standards, digital data formats, equipment standards, and design standards."* *– National Incident Management System*			
This product adheres to the principle of plain language (clear text).	Disagree	Agree	N/A
	☐	☐	☐
If not, cite examples.			
Incident reporting and documentation procedures are standardized to ensure that situational awareness is maintained and provides emergency management/response personnel with easy access to critical information.	Disagree	Agree	N/A
	☐	☐	☐
This product allows FEMA ICS forms to be completed.	Disagree	Agree	N/A
	☐	☐	☐
Comment on ICS forms.			
This product provides adequate access to critical information.	Disagree	Agree	N/A
	☐	☐	☐
Describe any issues with access to critical information.			
This product provides a method for data sharing or interoperability.	Disagree	Agree	N/A
	☐	☐	☐

Identify any deficiencies in data sharing.			
This product does not have potential security or vulnerability concerns.	Disagree	Agree	N/A
	☐	☐	☐
Identify any security or vulnerability concerns.			
Identify any safeguards taken to minimize security and/or vulnerability concerns.			
The system provides adequate controls to restrict access to sensitive information.	Disagree	Agree	N/A
	☐	☐	☐
COMMAND AND MANAGEMENT *" --- enable effective and efficient incident management and coordination by providing flexible, standardized incident management structures." – National Incident Management System*			
This product assists users in the management of an incident.	Disagree	Agree	N/A
	☐	☐	☐
This product supports (or is consistent with) the 14 management characteristics of ICS:	Disagree	Agree	N/A
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	☐	☐	☐
The organizational charts and/or terminology used in the product are consistent with Incident Command.	Disagree	Agree	N/A
	☐	☐	☐
Identify any inconsistencies with the management characteristics of ICS.			
IMPLEMENTATION AND PRODUCT OVERVIEW *NIMS leverages science and technology to improve capabilities and lower costs. It observes the five key principles: Interoperability and Compatibility, Technology and Support, Technology Standards, Broad-based Requirements, and Strategic Planning for R&D – National Incident Management System*			
IMPLEMENTATION			
This product can be easily implemented.	Disagree	Agree	N/A
	☐	☐	☐
System documentation (including training materials and user's guides) is comprehensive.	Disagree	Agree	N/A
	☐	☐	☐
Identify the type of training available for the average practitioner (e.g. online, train the trainer, etc.).			
Is an integrated help tool available? If so, is it adequate/intuitive?			
Is customer support available? If so, what is its availability and what medium is used (e.g. e-mail, phone, live-chat, etc.)?			
How long would it take a department or agency to implement this product (installation to proficiency)?			
The size or make up of the department or agency will affect the implementation of this product.	Disagree	Agree	N/A
	☐	☐	☐
If agree, comment.			

Training provided allows recipients to proficiently use this product.	Disagree	Agree	N/A
	☐	☐	☐
There are no other obstacles that would prohibit a department or agency from providing the training to implement this product.	Disagree	Agree	N/A
	☐	☐	☐
Identify any obstacles to training.			
Federal, state, or local laws or regulations will not hinder the implementation of this product.	Disagree	Agree	N/A
	☐	☐	☐
If so, describe how.			
The impact of implementing this product will not vary for urban vs. rural jurisdictions.	Disagree	Agree	N/A
	☐	☐	☐
If so, describe how.			
The impact of implementing this product will not vary for paid, combination, or volunteer departments.	Disagree	Agree	N/A
	☐	☐	☐
If so, describe how.			
Provide an estimate of the cost of this product (optional).			
Provide an estimate of associated costs that may be incurred in addition to the procurement of this product (staffing, etc.).			
PRODUCT OVERVIEW			
Overall, this product is consistent with the concepts and principles of the NIMS.	Disagree	Agree	N/A
	☐	☐	☐
Identify any inconsistencies.			
This product will enhance the user's ability to do his/her job.	Disagree	Agree	N/A
	☐	☐	☐
If so, describe how.			

This product was easy to use and intuitive.	Disagree	Agree	N/A
	☐	☐	☐
Identify any issues.			
This product was reliable during the evaluation.	Disagree	Agree	N/A
	☐	☐	☐
Identify any issues with reliability.			
Provide any other observations.			

APPENDIX E: REFERENCES

1. OASIS Standard CAP-v1.1, October 2005.
2. OASIS Standard EDXL-DE v1.0, May 2006.
3. National Incident Management System Document. FEMA 501 Draft, August 2007.
4. National Response Framework, January 2008.
5. NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.
6. NIMS Recommended Standard List,

   http://www.fema.gov/emergency/nims/nims_standards.shtm, January 2008.

APPENDIX F: ACRONYMS AND ABBREVIATIONS

ADA	Americans with Disabilities Act
CAP	Common Alerting Protocol
DCS	Data Collection System
DE	Distribution Element (EDXL Standard)
DHS	Department of Homeland Security
DMIS	Disaster Management Interoperability Services
EDXL	Emergency Data eXchange Language
EKU	Eastern Kentucky University
EOC	Emergency Operations Center
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GHIS	G&H International Services
GIS	Geographic Information Systems
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
ICS	Incident Command System
IMSI	Incident Management Systems Integration
IT	Information Technology
MIME	Multipurpose Internet Mail Extensions
N/A	Not Applicable
NDA	Non-Disclosure Agreement
NFPA	National Fire Protection Association
NGO	Non-Governmental Organizations
NIC	National Integration Center
NIMS	National Incident Management System
NIMS SC	National Incident Management System Support Center

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
RAM	Random-Access Memory
RFP	Requests for Proposal
RKB	Responder Knowledge Base
SAIC	Science Applications International Corporation
SAVER	System Assessment and Validation for Emergency Responders
SME	Subject Matter Expert
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
T&E	Test and Evaluation
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	eXtensible Markup Language