NIMS STEP Inspection Report

FirePrograms RMS version X.3 (10.3.8.35)

February 2011

FEMA

Table of Contents

List of Figures

List of Tables

Executive Summary

This report presents the results from an evaluation of FirePrograms Software's system[1], FirePrograms RMS version X.3 (10.3.8.35), herein referred to as FirePrograms. This evaluation was managed by the Federal Emergency Management Agency (FEMA) and was conducted from 8 through 11 November 2010 as part of the National Incident Management System Supporting Technology Evaluation Program (NIMS STEP).

This was a Comprehensive National Incident Management System (NIMS) Evaluation; and therefore, it specifically addresses adherence to NIMS concepts and principles. The evaluation does not address NIMS recommended technical standards. This evaluation had two 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).

FirePrograms is a software suite utilized by fire departments to operate and manage their operations and back-end office business system. FirePrograms utilizes the following modules:

- Station Manager is a National Fire Incident Reporting System (NFIRS) incident reporting package that allows the department to manage and organize their administrative procedures.
- Risk Manager provides the department with the means to track and manage information on the properties that they protect.
- The National Emergency Management System Information System (NEMSIS) Manager module is the primary module for entering Electronic Patient Care Reports (ePCRs).
- The Mobility module is an interface designed for in the field use with tablet PCs and laptops that run the Windows operating system.

The following features are common to all of the FirePrograms modules: Geographic Information System (GIS) mapping, calendar functions with linked icons, Email (Internal and External), database search, and over 300 built-in reports and various custom reporting capabilities.

Participants received two days of training on-site with a professional trainer for FirePrograms. While on-site at the Incident Management Test and Evaluation Laboratory (IMTEL[2]), the vendor demonstrated the installation process in preparation for the evaluation. It took approximately two hours to install FirePrograms on five systems. Each participant was provided with an electronic copy of the user guide for FirePrograms.

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 FirePrograms based on concepts and

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

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

principles from the NIMS document (December 2008). Assessors also identified which of the core capabilities from the TCL (September 2007) applied to the product.

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**)	5	1	3
Resource Management (**10**)	3	0	7
Command and Management (**2**)	1	0	1

Note: A description of the NIMS criteria and Minimum Product Requirements is provided in Appendix A.

FirePrograms is consistent with all applicable NIMS criteria. Overall, FirePrograms applies to 13 of 24 Minimum Product Requirements; all of which 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:

FirePrograms 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). FirePrograms applies to 7 of 15 ESFs and it is applicable to 7 of 9 Incident Command functions (see Emergency Support in **Table 6: NIMS STEP Worksheet**). One item that will impact users is the need to manually pre-load data. However, in certain circumstances, the vendor can bulk-load existing data into the system (e.g., fleet information, equipment, personnel) from other RMS software vendors on a case-by-case basis.

Hazards:

FirePrograms 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 as well as human- and technological-caused events.

Preparedness:

FirePrograms meets the Minimum Product Requirement for Preparedness as the system can be used to support at least one of the core preparedness activities. FirePrograms can be used to support planning; training and exercises; Personnel Qualifications, Licensure, and Certification; and Equipment Certification. The system provides a repository for the data required for developing fire pre-plans.

Communications and Information Management:

FirePrograms meets 6 of 9 Minimum Product Requirements for Communications and Information Management. As an incident reporting system, FirePrograms can be used in small- and large-scale incidents and events, in single jurisdictions, and during multi-agency incidents and events. However, FirePrograms is not designed to share data with other systems and does not provide situational awareness during an incident. The system is focused on pre- and post-incident information management. Additionally, it can be used across the full spectrum of multi-discipline incidents and events.

In general, FirePrograms does support plain language (clear text); however, there are a limited number of proprietary acronyms that are not defined.

FirePrograms provides a means to authenticate and certify users for security purposes; however, issues were identified regarding user login and password requirements. The system allows user login requirements to be turned off and does not enforce requirements on passwords (complexity, length, characters, etc.).

Resource Management:

FirePrograms meets 3 of 10 Minimum Product Requirements for Resource Management. The system provides a means for inventorying non-FEMA typed resources, can provide a record of credentialed and other personnel, and can assist in the reimbursement process. FirePrograms equipment and personnel accountability is not suited to real-time emergency response and is more useful in a post-event/incident reporting environment.

Command and Management:

FirePrograms meets 1 of 2 Minimum Product Requirements for Command and Management. The system is consistent with 2 of 14 ICS management characteristics including Incident Action Planning, and Incident Facilities and Locations. FirePrograms does not use ICS organization charts or terminology.

Implementation Considerations:

FirePrograms can be easily implemented; however, to maximize the value of the system the user must preload a significant amount of information. On-site training is not part of the standard package but it is

available for an additional cost. FirePrograms includes an electronic user guide as part of the system but there is no integrated help tool.

Target Capabilities List

FirePrograms applies to core capabilities that address: response 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.

1.0 Introduction

This report presents the results from an evaluation of FirePrograms Software's system FirePrograms RMS version X.3. 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 hardware[3] 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.).

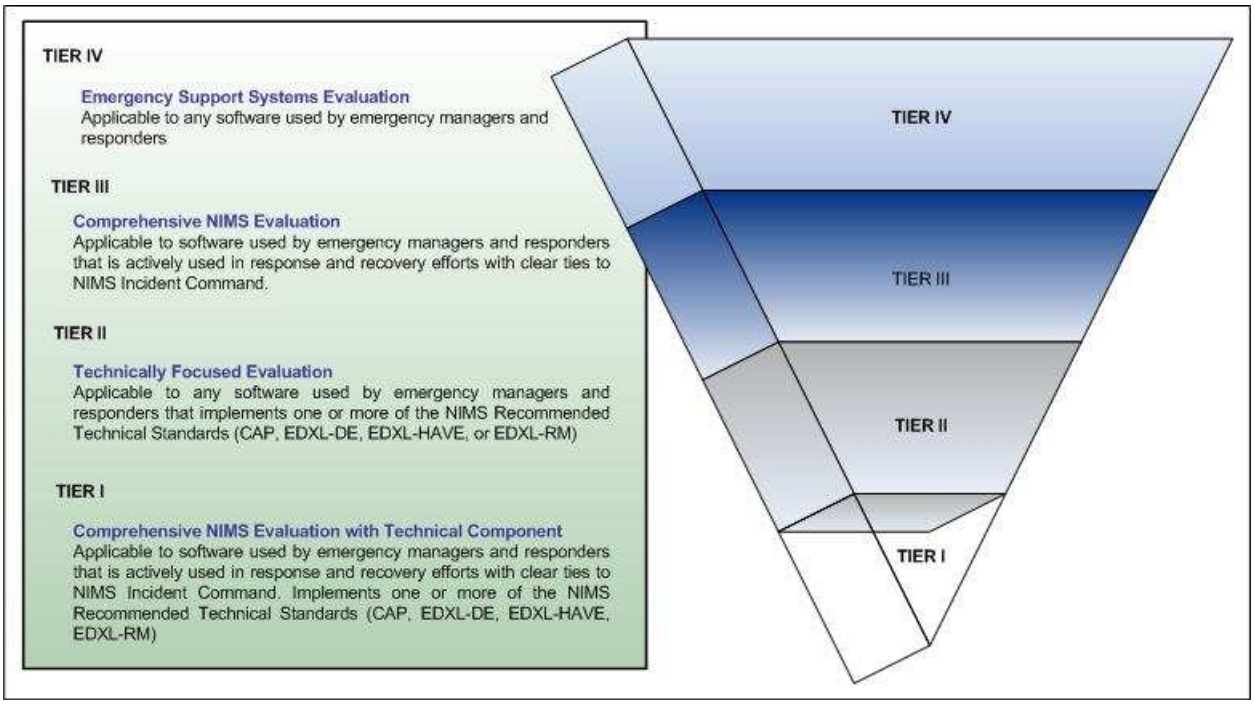

Figure 1: Tiered Evaluation Approach

A Tier III–Comprehensive NIMS Evaluation was conducted for FirePrograms. The intent of this evaluation was to determine the system's ability to incorporate NIMS concepts and principles.

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, simulated EOC-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. 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 Description[4]

FirePrograms is a software suite utilized by fire departments to operate and manage their operations and back-end office business system. The following is a description of the major modules of FirePrograms Records Management System (RMS):

Station Manager is an incident reporting package that allows the department to manage and organize their administrative procedures including the ability to print standard, graphic and custom reports used to analyze resource allocation, justify additional resources or to support an ISO audit. The Station Manger module includes the following components: NFIRS compliant Incident Reporting, Personnel and Staff Management, Training Records, Apparatus Maintenance, Basic Life Support reporting (non-NEMSIS users), Apparatus Fleet and Equipment Inventory with bar coding.

Risk Manager provides the department with the means to track and manage information on the properties that they protect. Like Station Manager, this fully integrated package can be used at one station or over a Wide Area Network of multiple stations or offices. The Risk Manager module contains the following components: Locations and Property Records, Pre-Plans, Permits, Hazardous Materials (HAZMAT), Hydrant Locations Testing and Inspections, Inspections and Code Enforcement.

NEMSIS Manager is a NEMSIS gold certified module for entering ePCRs. This module allows the department to manage all of their Emergency Medical Services (EMS) reporting for compliance at both state and national levels. The module allows EMS personnel to document patient details such as treatment, transport and transfer of care when the patient arrives at the hospital.

[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.

Mobility Module is an interface designed for use in the field with tablet PCs and laptops that run the Windows operating system. The interface provides the ability to enter and look up data while on scene, regardless of whether they have a communications connection.

The following features are common to all of the FirePrograms modules: GIS mapping, calendar functions with linked icons, Email (Internal and External), database search, and over 300 built in reports and various custom reporting capabilities.

Figure 2: depicts the default desktop environment for FirePrograms.

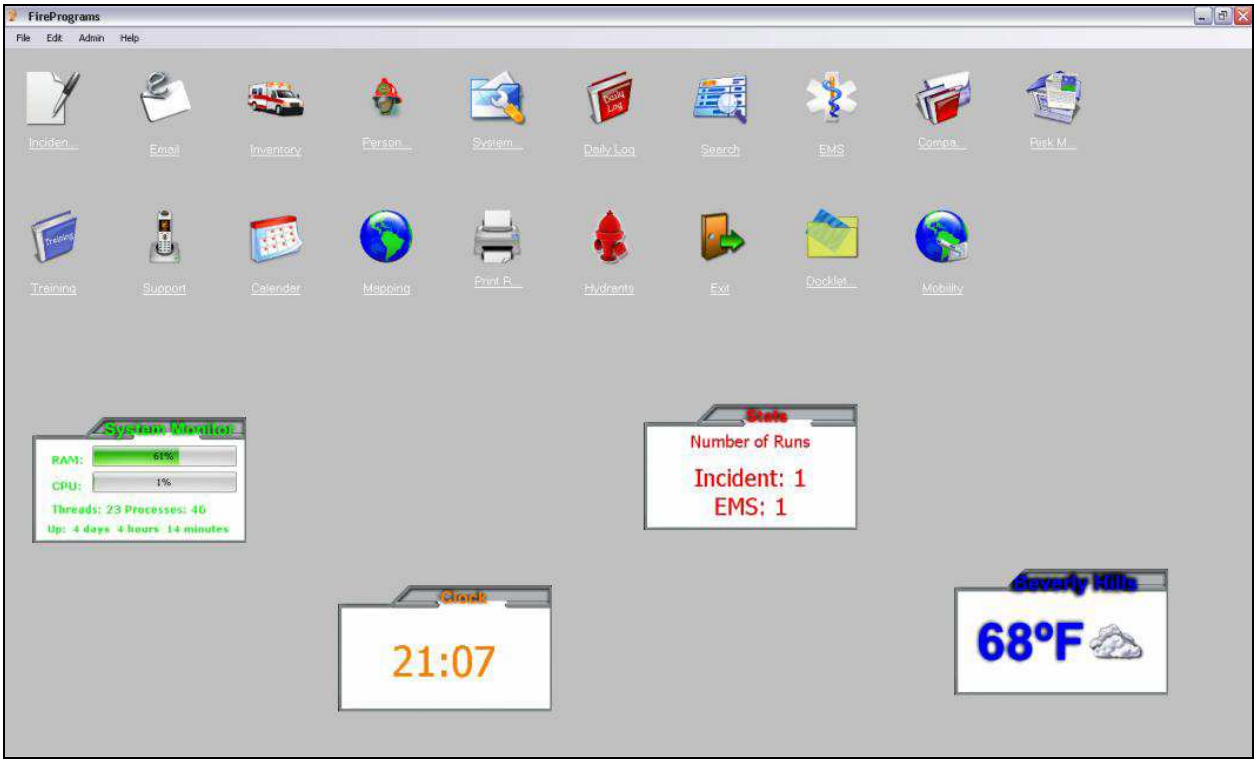

Figure 2: FirePrograms Desktop

The default desktop of FirePrograms has preset icons to open the menus for FirePrograms modules, including: Mobility, Docklet Manager, Incident Reporting, Print Reports, Mapping, Calendar, Hydrants, Support, Training, Risk Manager, Company Report, EMS, Search, Daily Log, System Setup, Personnel, Inventory, Email, and Exit. These icons can be rearranged, changed or deleted and new ones can be created by users.

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 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.

1.4 Evaluation Setup

The evaluation was conducted on site at the IMTEL. The vendor provided multiple licensed installations for IMTEL workstations and provided usernames/passwords to allow complete access to the system during the evaluation. A test engineer managed the test environment, and was available to assist the vendor in resolving any technical issues.

1.5 Evaluation Schedule

The NIMS STEP team conducted the FirePrograms evaluation from 8 through 11 November. **Table 3: Evaluation Schedule** provides a summary of key events and milestones.

Table 3: Evaluation Schedule

Event	Date(s) 2010
Evaluation Readiness Review (ERR)	29 October
Administrative system setup and pre-evaluation checks	8 November
Participant training	8-9 November
Rehearsal of system evaluation procedures	10 November

[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]).

Evaluation execution	10-11 November
Data analysis and Quality Control (QC)	11 November

On 29 October, the NIMS STEP team conducted an ERR to ensure logistic and technical preparations were complete. The vendor provided participants with two days of on-site training (presentation, demonstration, and hands on) from 8 through 9 November. The participants evaluated the system on 10 and 11 November.

1.6 Scope and Limitations

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

Table 4: Scope and Limitations

Limitation	Impact	Mitigation Strategy
None identified.	NA	NA

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 Engineer	Emergency Response Assessor, NIMS Inspection (Experience: Medical, Firefighting, Emergency Management)	34
Technical Information Specialist	Emergency Response Assessor, NIMS Inspection (Experience: Medical, Firefighting, Law Enforcement, Emergency Management)	25
Systems Engineer	Test Analyst	17
Test Engineer	Test Engineer	17
Test and Evaluation Analyst	Test Analyst	3

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. The following sections describe the approach to the evaluation in more detail.

2.2.1 NIMS Inspection and TCL Identification

After receiving information from the vendor, the lead assessor developed a hurricane scenario to effectively exercise FirePrograms' capabilities. 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 FirePrograms, 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 FirePrograms, 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.

2.3 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, 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. All FirePrograms software was removed from IMTEL systems after the evaluation was concluded.

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 FirePrograms to determine if the system incorporates NIMS concepts and principles, and documented results as identified in the following sections for Objective 1.

FirePrograms is consistent with all 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

FirePrograms applies to 7 ESFs (Firefighting; Emergency Management; Logistics Management and Resource Support; Public Health and Medical Services; Search and Rescue; Oil and Hazardous Materials Response; and Public Safety and Security). FirePrograms applies to 7 of 9 Incident Command functions (Incident Command, Operations, Planning, Logistics, Finance/Administration, Intelligence/Investigations, and Safety). With regard to the direct and indirect support requirements of Incident Command functions implementing this product; the system does not provide a capability to bulk-load existing data into the system (e.g., fleet information, equipment, personnel), which greatly increases the time required to set up the product's database prior to use.

3.1.1.2 Hazards

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

3.1.1.3 Preparedness[6]

FirePrograms can be used to effectively support the preparedness activities for planning; training and exercises; personnel qualifications, licensure, and certification; and equipment certification. The system provides a repository of data required for developing fire pre-plans.

3.1.1.4 Communications and Information Management

Common Operating Picture:

FirePrograms provides access to critical information and uses or interacts with geospatial information to portray the incident. The system is not designed to provide a common operating picture; it is designed to be a post-incident reporting tool.

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

Interoperability:

FirePrograms is not designed to provide situational awareness during an incident. The system is not designed to share data with other incident management systems; however, it does provide a method to provide NFIRS data to country or state entities after an incident.

Scalability:

FirePrograms can be used for small- and large-scale events and is flexible and scalable to support the full spectrum of multi-agency incidents and events. The system applies to multiple levels of the government and to the public and private sector. Scalability may be impacted by the fact that the system is designed as a reporting tool specific to the responders function in the venue and the Mobility module restricts synchronization to a single user at a time.

Plain Language:

In general, FirePrograms does support plain language (clear text); however, there are a limited number of proprietary acronyms that are not defined.

Information Security:

FirePrograms requires usernames and passwords to log into the system and users are assigned roles/permissions. However, due to the lack of strong login requirements (e.g., complexity, length, special characters) combined with the capability to turn-off login requirements there are potential security concerns. With security requirements disabled there is the potential that unauthorized users could access private information. Users implementing this system should carefully apply and understand this feature to meet their organization's security needs.

3.1.1.5 Resource Management

FirePrograms addresses the need to manage resources. The product allows for the inventory of non-FEMA typed resources prior to an incident or event. The product also provides a record of credentialed and other personnel. Furthermore, the product can assist in the reimbursement process.

3.1.1.6 Command and Management

FirePrograms is consistent with 2 of 14 management characteristics of the Incident Command System (ICS): Incident Action Planning; and Incident Facilities and Locations.

3.1.1.7 Implementation and Product Overview

The primary capability of FirePrograms is that it is an incident reporting tool. It should take less than three months for a department/agency to implement FirePrograms (from acquiring and installation to user proficiency). The system's user guide is comprehensive; however, FirePrograms does not have an integrated help tool. The vendor offers online, train-the-trainer, on-site presentation and hands-on training. On-site training is available for an additional cost; it is comprehensive and allows recipients to proficiently use the system. Customer support is available by telephone, email, and live chat. The primary impact to implementation is data integration; departments could be impacted by the time required to preload data.

FirePrograms 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. When errors were encountered while using the system, selecting "More information" provided a support 800 number and some details to assist customer support in resolving the issue; however, **Figure 3: FirePrograms Error** provides an example of how error messages were generic and provided no direct guidance to the user, such as what issue was encountered or what user actions could correct the issue.

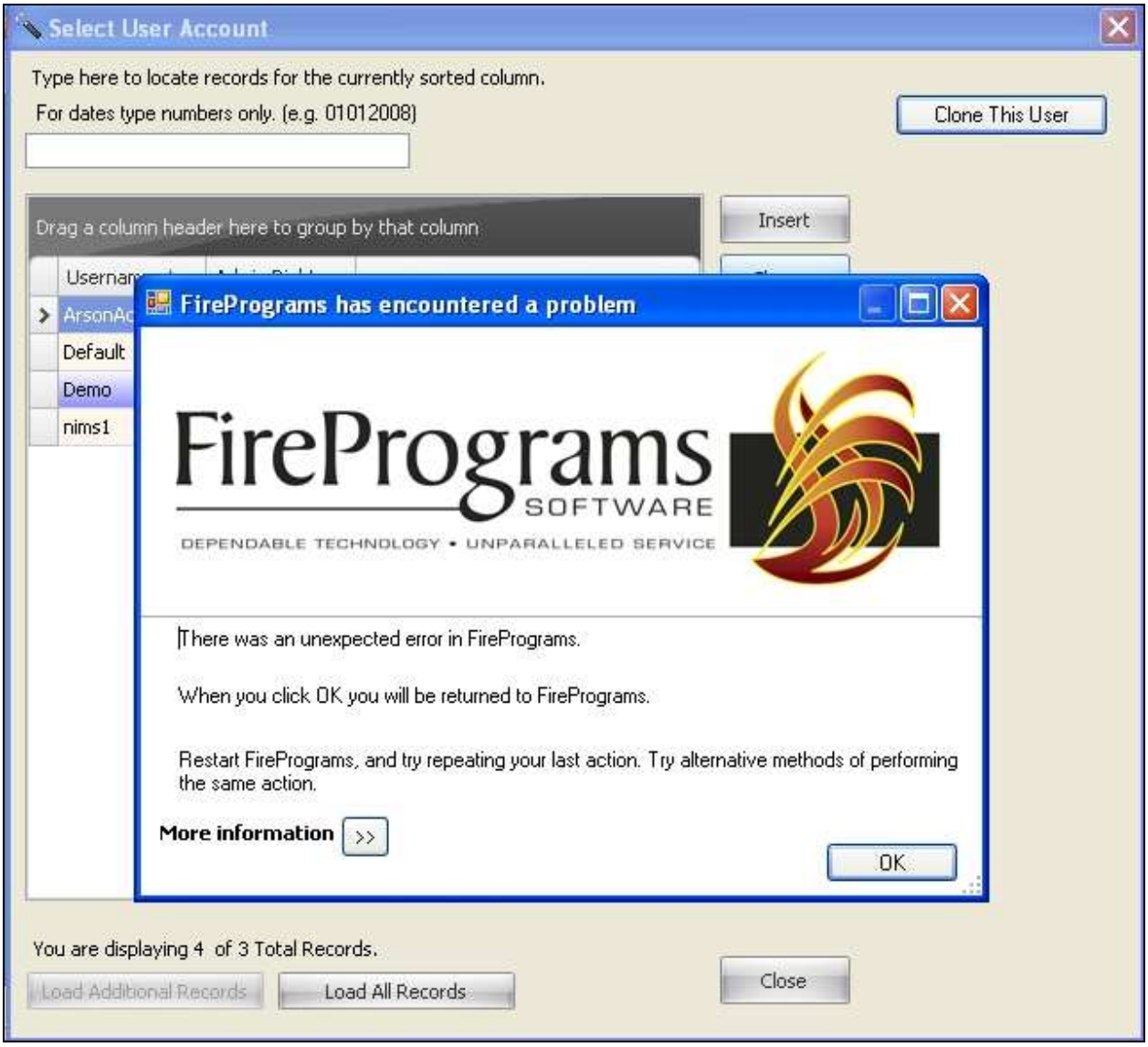

Figure 3: FirePrograms Error

3.1.1.8 NIMS STEP Worksheet

Table 6: NIMS STEP Worksheet provides specific details of the evaluation results.

Table 6: 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	Not Applicable
b. ESF #2 - Communications	Not Applicable
c. ESF #3 - Public Works and Engineering	Not Applicable
d. ESF #4 – Firefighting	Agree
e. ESF #5 - Emergency Management	Agree
f. ESF #6 - Mass Care, Emergency Assistance, Housing, and Human Services	Not Applicable
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	Not Applicable
l. ESF #12 – Energy	Not Applicable
m. ESF #13 - Public Safety and Security	Agree
n. ESF #14 - Long-Term Community Recovery	Not Applicable
o. ESF #15 - External Affairs	Not Applicable
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.	None identified.
INCIDENT COMMAND	
4. This product supports the following Incident Command functions:	Agree/Disagree/Not Applicable
a. Incident Command	Agree
b. Operations	Agree
c. Planning	Agree
d. Logistics	Agree
e. Finance/Administration	Agree

f. Intelligence/Investigations	Agree
g. Public Information	Not Applicable
h. Safety	Agree
i. Liaison	Not Applicable
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 system does not provide a capability to bulk load existing data into the system (e.g., fleet information, equipment, personnel).
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. Natural hazards	Agree
b. Human-caused events	Agree
c. Technological-caused events	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. Planning	Agree
b. Procedures and Protocols	Not Applicable
c. Training and Exercises	Agree
d. Personnel Qualifications, Licensure, and Certification	Agree
e. Equipment Certification	Agree
f. Evaluation and Revision	Not Applicable

12. Provide comments on the product's support to preparedness activities.	They system provides a repository for the data required for developing fire pre-plans.
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).	Not Applicable
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.	Not Applicable
17. This product has the capability to be updated continually in order to maintain situational awareness.	Not Applicable
18. This product uses or interacts with geospatial information to portray the incident.	Agree
19. Provide comments on the common operating picture.	This product is not designed to provide a common operating picture; it is designed to be a post-incident reporting tool.
INTEROPERABILITY	
	Agree/Disagree/Not Applicable
20. Incident reporting and documentation procedures are standardized to ensure situational awareness.	Not Applicable
21. Comment on incident reporting and documentation procedures.	This product is not designed to provide situational awareness during the incident.
22. This product allows NIMS ICS forms to be completed.	Not Applicable
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)**	Not Applicable

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 is
a. *Swap Files*	Not Applicable
b. *Common Applications*	Not Applicable
c. *Custom-Interfaced Applications*	Not Applicable
d. *One-Way Standards-Based Sharing*	Not Applicable
e. *Two-Way Standards-Based Sharing*	Not Applicable
26. Provide comments on data sharing.	The product is not designed to share data with other incident management systems, however; it does provide a method to provide NFIRS data to county or state entities. The NEMSIS Manager portion of the system allows users to enter ePCRs.
27. This product is interoperable with other systems at the level of c, d, or e above. **(Minimum Product Requirement 5)**	Not Applicable
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)**	Not Applicable
33. This product allows responders to increase the number of users on a system.	Agree

34. Provide comments on scalability.	29, 31, and 32: The product is intended as a reporting tool specific to the responders function in the venue. 33: The system is based on the number of concurrent user licenses purchased. Multiple users cannot synchronize simultaneously.
35. The product can be used at the following:	Agree/Disagree/Not Applicable
a. On scene as a portable or static device.	Agree
b. On scene at the Incident Command Post (ICP).	Agree
c. At a Staging Area, Base, or Camp.	Agree
d. At a local EOC.	Agree
e. At a state EOC.	Not Applicable
f. At a Federal Joint Field Office (JFO) or EOC.	Not Applicable
36. Provide comments on Command and Coordination levels.	The product's primary function is a reporting tool.
37. This product can be used by the following levels of government:	Agree/Disagree/Not Applicable
a. Municipality	Agree
b. County	Agree
c. Regional	Agree
d. Tribal	Agree
e. State	Agree
f. Federal	Agree
g. Special District	Agree
h. Agency	Agree
i. Other	Agree
38. This product can be used to support communications among multiple levels of government(s).	Not Applicable
39. Provide comments on levels of government.	The software is applicable to any level of government that is providing fire response or EMS assets.
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.	In general, FirePrograms does support plain language (clear text); however, there are a limited number of proprietary acronyms that are not defined.
INFORMATION SECURITY	
	Agree/Disagree/Not Applicable
44. This product has redundancy capabilities as a part of its functionality.	Agree
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.	Disagree
48. Describe any safeguards integrated to minimize security and/or vulnerability concerns.	The system provides for login and password. However, the system does not utilize strong password requirements.
49. Provide comments on Information Security.	Due to the lack of strong password requirements or login requirement the system creates a potential security concern as it can allow unauthorized users access to private information. Users implementing this system should carefully apply and understand this feature to meet their organization's security needs.
Minimum Product Requirement Summary: Rating for the Communications and Information Management category.	**Agree:** 5 of 9 **Disagree:** 1 of 9 **Not Applicable:** 3 of 9

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.	Not Applicable
52. This product provides for mobilizing resources.	Not Applicable
53. This product addresses the use of Mutual Aid Agreements and resources. **(Minimum Product Requirement 13)**	Not Applicable
54. This product provides an integrated means for resource typing definitions. **(Minimum Product Requirement 14)**	Not Applicable
55. This product provides a means for inventorying FEMA typed resources. **(Minimum Product Requirement 15)**	Not Applicable
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)**	Not Applicable
59. This product provides a means for resource requesting/ordering. **(Minimum Product Requirement 19)**	Not Applicable
60. This product provides a means for resource tracking/reporting. **(Minimum Product Requirement 20)**	Not Applicable
61. This product provides a means for resource recovery and demobilization. **(Minimum Product Requirement 21)**	Not Applicable
62. This product assists in the reimbursement process. **(Minimum Product Requirement 22)**	Agree
63. Provide comments on resource management.	58: The system provides equipment and personnel accountability on a non-emergency basis. 60: The system provides a means for resource reporting.

Minimum Product Requirement Summary: Ratings for the Resource Management category.	**Agree:** 3 of 10 **Disagree:** 0 of 10 **Not Applicable:** 7 of 10

COMMAND AND MANAGEMENT

Criteria and Question	Result
	Agree/Disagree/Not Applicable
64. This product assists users in the management of an incident.	Not Applicable
65. This product supports (or is consistent with) the following management characteristics of ICS:	Agree/Disagree/Not Applicable
a. Common Terminology	Not Applicable
b. Modular Organization	Not Applicable
c. Management by Objectives	Not Applicable
d. Incident Action Planning	Agree
e. Manageable Span of Control	Not Applicable
f. Incident Facilities and Locations	Agree
g. Comprehensive Resource Management	Not Applicable
h. Integrated Communications	Not Applicable
i. Establishment and Transfer of Command	Not Applicable
j. Chain of Command and Unity of Command	Not Applicable
k. Unified Command	Not Applicable
l. Accountability	Not Applicable
m. Dispatch/Deployment	Not Applicable
n. Information and Intelligence Management	Not Applicable
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)**	Not Applicable
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:** 1 of 2 **Disagree:** 0 of 2 **Not Applicable:** 1 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.	The user must preload a significant amount of information.
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. Online	Agree
b. Train the trainer	Agree
c. On-site presentation	Agree
d. Hands-on training	Agree
73. Comment on practitioner training.	On-site training is not part of the standard package; however, it is available for an additional cost.
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.	Disagree
78. Comment on the help tool.	There is no integrated help tool in the software.
79. Is customer support available? If so, what is its availability and what medium is used (e.g., e-mail, phone, live-chat)?	Customer support is available via telephone, e-mail and live-chat.
80. How long would it take a department, agency, or jurisdiction to implement this product?	Less than three months.
81. Comment on how the size or make up of a department, agency, or jurisdiction can impact the implementation of this product.	The primary impact to implementation is data integration.

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.	None identified.
86. Identify any issues with paid, combination, or volunteer departments.	Departments could be impacted by the time required to preload data.
87. Identify associated expenditures that may be incurred in addition to the initial procurement of this product.	None identified.
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.	This product is focused on incident reporting and not incident management. Therefore, it is focused on a limited number of NIMS concepts and principles.
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.	None identified.
92. This product was easy to use and intuitive.	Agree
93. Comment on the products ease of use.	Error messages were generic and provided no direct guidance to the user, such as what issue was encountered or what user actions can correct the issue.
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 is primarily an incident reporting tool.
97. Provide any other observations.	None identified.

3.2 TCL

3.2.1 Objective 2: Identify Applicable TCL Core Capabilities[7]

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

Common Capabilities:

- Planning
- Risk Management
- Intelligence and Information Sharing and Dissemination

Respond Mission Capabilities:

- Critical Resource Logistics and Distribution
- Responder Safety and Health
- Fire Incident Response Support
- Weapons of Mass Destruction (WMD) and Hazardous Materials Response and Decontamination
- Search and Rescue (Land-Based)
- Emergency Triage and Pre-Hospital Treatment

3.3 Participant Observations

- Data Entry and User Interface
    - Assessors attempted to enter data in various screens and received error messages which interfered with ease of use. Generally shutting-down/restarting would resolve these issues.
    - **Figure 4: Fast Shutdown/Restart Sharing Violation** shows the popup window generated when assessors attempted to shut-down then quickly restart the system. The vendor stated that this is not a typical user action and that the SQL database requires three to eight seconds to complete the shut down process.

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

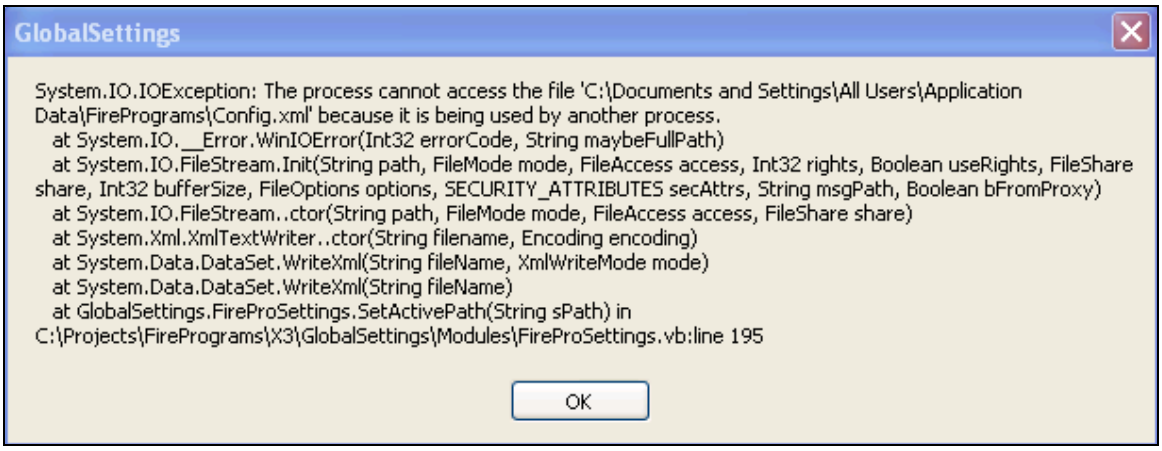

Figure 4: Fast Shutdown/Restart Sharing Violation

- **Figure 5: Finish Later Error** shows an error that occurred when assessors attempted to finish an Incident Report later by clicking the "Finish Later" button. The vendor stated that NFIRS requires certain fields to be numeric-only data and that the use of the alphanumeric "3a" in this field is what caused the error.

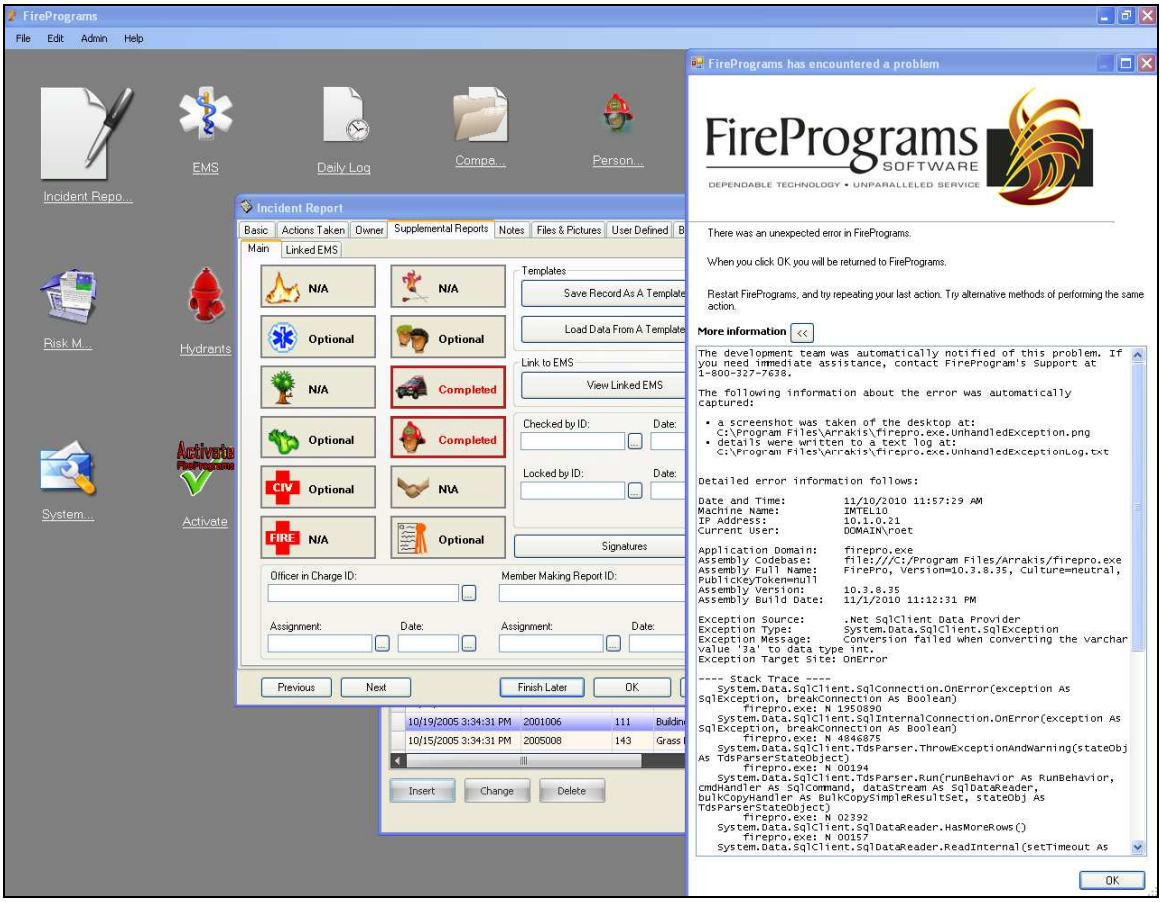

Figure 5: Finish Later Error

- There were numerous errors generated when users moved from section to section of the various modules; this may have been avoided if a different sequence had been followed.

4.0 Appendix A: 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 (SMEs) 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 7: NIMS Criteria Rating Summary** is included 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 7: 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 in **Table 8: 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 8: 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

Reference Number	Minimum Product Requirements Text	NIMS Criteria
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
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 National Response Framework (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 interoperability[8], 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.

[8] 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).

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.

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: 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 9: 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 9: Core Target Capabilities Form

Core Target Capability	Supported By Product
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	
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	
Respond Mission Capabilities	
Structural Damage Assessment	
Restoration of Lifelines	
Economic and Community Recovery	

6.0 Appendix C: References

1. A2LA, http://www.a2la.org/.
2. FirePrograms Software Website, http://www.fireprograms.com/index.html, accessed December 2010.
3. National Incident Management System, December 2008, http://www.fema.gov/emergency/nims/.
4. National Response Framework, January 2008, http://www.fema.gov/emergency/nrf/.
5. National Fire Protection Association (NFPA) 1600: Standard on Disaster/Emergency Management and Business Continuity Programs, 2007, http://www.nfpa.org/.
6. National Incident Management System (NIMS) Recommended Standard List, January 2009 http://www.fema.gov/pdf/emergency/nims/FY09_Recommend_Standards_List_121708.pdf.
7. National Incident Management System Supporting Technology Evaluation Program (NIMS STEP): FirePrograms RMS Evaluation Plan, October 2010.
8. NIMS STEP Guide, September 2010.
9. SAFECOM Interoperability Continuum, accessed October 2009, http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf.
10. Target Capabilities List (TCL), September 2007, http://www.fema.gov/pdf/government/training/tcl.pdf.

7.0 Appendix D: List of Acronyms and Abbreviations

A2LA	American Association for Laboratory Accreditation
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
DCS	Data Collection System
DHS	Department of Homeland Security
EOC	Emergency Operations Center
EMS	Emergency Medical Services
ePCR	Electronic Patient Care Report
ERR	Evaluation Readiness Review
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
HAZMAT	Hazardous Materials
HIPPA	Health Insurance Portability and Accountability Act
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
NEMSIS	National Emergency Management System Information System
NFIRS	National Fire Incident Reporting System

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
QC	Quality Control
SAIC	Science Applications International Corporation
SME	Subject Matter Expert
T&E	Test and Evaluation
TCL	Target Capabilities List
UC	Unified Command
WMD	Weapons of Mass Destruction