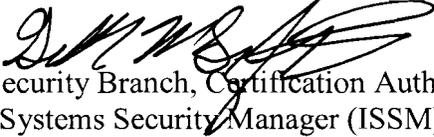




FEMA

JUL 30 2007

MEMORANDUM FOR: Stan Stewart  
System Owner, National Fire Incident Reporting System

THROUGH: Gerald Singleton   
Acting Chief, IT Security Branch, Certification Authority  
(CA)/Information Systems Security Manager (ISSM)

FROM: Anthony T. Cirone   
Chief Information Officer/Director, Information Technology  
Services Division  
Designated Approving Authority (DAA)

SUBJECT: System Security Accreditation of the National Fire Incident  
Reporting System

1. I hereby grant authority to operate the National Fire Incident Reporting System for a period of six months from the date signed below. This accreditation is based upon my review of the Certification Authority's recommendation after review of technical vulnerability assessment results.
2. It is my assessment that due diligence for the appropriate system security countermeasures are being addressed and the risk to FEMA LAN/WAN is moderate due to the lack of completed security documentation. I understand and accept these risks.
3. This accreditation is based on the system and information classification, security mode of operation, threats, vulnerabilities, countermeasures, residual risk, mission/system description, concept of operation, operating environment, and interconnections identified in the System Security Plan. Any change to those factors may lead to my future disapproval for system operation. Therefore, it is incumbent upon the System Owner, Information System Security Officer (ISSO), and System Administrator to ensure that any changes in those factors are analyzed to determine the impact on system security. Accordingly, appropriate action must be taken to maintain the appropriate level of protection consistent with the requirements for this accreditation. The ISSO must develop a Plan of Action and Milestone to address the finalization of a documentation and resolution of any vulnerabilities noted during the security assessment of this system within the time period granted by the letter. This requirement consists of but not limited to the System Security Plan, Risk Assessment, Contingency Plan, Results of Contingency Plan Test, System Test and Evaluation

Plan, Security Assessment Report, or other documents required by DHS Sensitive Security Systems Handbook 4300A and completed with the DHS approved Risk Management System (RMS) tool. These requirements are also established by OMB Circular A-130, Appendix III and security controls (as categorized by FIPS 199) in NIST Special Publications 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* and 800-53 Rev 1, *Recommended Security Controls for Federal Information Systems*.

4. This accreditation is valid for not more six months from the date of this letter. It is the responsibility of the ISSO to ensure that reaccreditation is initiated sooner if there is a change affecting the system security posture.

Please return a signed copy of this National Fire Incident Reporting System Accreditation Decision Letter to IT Security Branch, Attention: Richard Steadman, Bldg 429, Mount Weather. Questions should be directed to Richard Steadman, (540) 542-2376.

Signed,

\_\_\_\_\_ Date: \_\_\_\_\_

Anthony T. Cira  
Chief Information Officer/Director, Information Technology Services Division  
Designated Accrediting Authority (DAA)

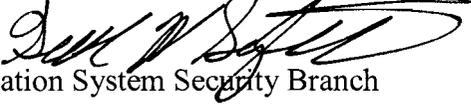
cc:  
Jackie Juliano, ISSO



FEMA

JUL 2 4 1

MEMORANDUM FOR: Anthony T. Cira  
Chief Information Officer/Director, Information Technology  
Services Division  
Designated Accrediting Authority (DAA)

FROM: Gerald M. Singleton   
Acting Chief, Information System Security Branch

SUBJECT: Certification Statement and Request for Accreditation of  
National Fire Incident Reporting System

1. I hereby recommend a six month accreditation to allow continued operation of the National Fire Incident Reporting System. This accreditation is based on the certification team's review and analysis of the Technical Vulnerability Assessment.
2. It is my assessment that due diligence for the appropriate system security countermeasures are being addressed and the risk to FEMA LAN/WAN is **moderate** due to the lack of completed security documentation. Contracting support is currently being solicited to mitigate this risk and completion of this task will be completed within the limits of the six month accreditation requested. Prior to the expiration of this ATO, another request will be issued for a full Authority to Operate when all requirements have been met.
3. The System Owner, Information System Security Officer (ISSO), and System Administrator must ensure that any changes in the current security posture are analyzed to determine the impact on system security. The ISSO must develop a Plan of Action and Milestone to address the finalization of a documentation and resolution of any remaining vulnerabilities noted during the security assessment of this system. This requirement consists of but not limited to the finalization of the System Security Plan, Risk Assessment, Contingency Plan, Results of Contingency Plan Test, System Test and Evaluation Plan, Security Assessment Report, or other documents required by DHS Sensitive Security Systems Handbook 4300A and completed with the DHS approved Risk Management System (RMS) tool. These requirements are also established by OMB Circular A-130, Appendix III and security controls (as categorized by FIPS 199) in NIST Special Publications 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* and 800-53 Rev 1, *Recommended Security Controls for Federal Information Systems*.

4. I certify that an appropriate level of technical protection exists and recommend that you sign the letter granting this accreditation.
5. I will ensure that this certification letter and the signed accreditation letter are maintained by the IT Security Branch, System Owner and the ISSO as required. Please return a signed copy of this letter to the IT Security Branch, Attention: Richard Steadman, Bldg 429, Mount Weather. By signing the National Fire Incident Reporting System Accreditation Assessment you acknowledge and accept any residual risk associated with the National Fire Incident Reporting System. Questions should be directed to Richard Steadman, telephone (540) 542-2376.

Signed,

\_\_\_\_\_ Date: \_\_\_\_\_  
Gerald M. Singleton  
Acting Chief, Information System Security Branch  
Certifying Official

Signed,

\_\_\_\_\_ Date: \_\_\_\_\_  
Anthony T. Cira  
Chief Information Officer/Director, Information Technology Services Division  
Designated Accrediting Authority (DAA)

cc:  
Rachel Offutt, ISSO