**Federal Emergency Management Agency**
**United States Fire Administration**
**National Fire Data Center**
**PHONE:** (301) 447-1353
**FAX:** (301) 447-1651
**USFA Website: www.usfa.fema.gov**

**TO:** **Vince Lisa**
**757-444-6044**

**FROM:** **Alex Furr, Division Director**
**National Fire Data Center**
**USFA/FEMA**

Subject: NFIRS accreditation

7 pages follow

# Federal Emergency Management Agency

Washington, D.C. 20472

JUL 11 2003

MEMORANDUM FOR: Dave Paulison
Director
Preparedness Division
Emergency Preparedness and Response

FROM: Rosita O. Parkes
Chief Information Officer

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

I'm sending this to you because you are the Designated Approving Authority for the National Fire Incident Reporting System. This memorandum provides the security certification statement by the Office of Cyber Security (OCS), Office of the Chief Information Officer (OCIO) and requests your decision concerning the formal security accreditation of the National Fire Incident Reporting System (NFIRS).

Based on attached system documentation required to certify NFIRS, I certify, with the exceptions or clarifications noted below, that this system appears to adequately meet federal and EP&R/FEMA policies, regulations and standards. In addition, test results demonstrated installed security safeguards appear to meet EP&R/FEMA business requirements and are appropriate for the sensitivity of the system and the information that it processes.

The certifying team, comprised of NFIRS technical staff, OCS and SAIC (under contract with OCS) conducted a *Level 4 Comprehensive Analysis*[1] that included reviewing existing system documentation, interviewing NFIRS staff, and conducting network and host security technical vulnerability assessments. The certifying team evaluated technical, management, and operational controls against defined EP&R/FEMA Baseline Security Requirements (BLSRs). Finally, the certifying team evaluated known vulnerabilities and suggested countermeasures that mitigate identified risks.

## FINDINGS

This section is a high-level analysis of the system threats, vulnerabilities, countermeasures, and mission impact to EP&R/FEMA and the NFIRS critical infrastructure in case of exploitation of vulnerabilities. The information is extracted from the recently conducted NFIRS Risk Assessment and presents any remaining risks. For the more detailed analysis and recommendations, refer to the *NFIRS Risk Assessment Report (Draft) August* 2002, reviewed and formally approved by OCS on March 2003.

---

[1] The level of certification is based upon the system's business function, national, departmental, and agency security requirements, criticality of the system to the organizational mission, software products, computer infrastructure, data processed, and user types with Level 4 being the most comprehensive and Level 1 being the most basic. (*NSTISSI No. 1000 April 2000 - NIACAP*)

**NFIRS Overall Security Risk**

After evaluation of risk level parameters (vulnerability, threat, countermeasures, mission impact) OCS concludes that the NFIRS overall security risk is considered ***low***.

**Vulnerability Findings**

Emphasis was placed on evaluating system deficiencies measured as technical, operational, or management vulnerabilities. Table 1 summarizes the findings.

**Table 1: NFIRS Vulnerability Findings**

| Risk Level | Vulnerabilities Found | | |
|---|---|---|---|
| | Technical | Operational | Management |
| High | 0 | 0 | 0 |
| Medium | 4 | 1 | 1 |
| Low | 7 | 1 | 0 |

**Medium Risk**

1. Risk: Resulting from lack of audit controls include failure to collect appropriate data in logs, failure to provide guidance on what should be audited and what the log reviews should cover, and lack of a routine procedure for reviewing logs weekly.

   Mitigation: Guidance for configuring and reviewing the audit trail is currently being drafted and will be included in the NFIRS Operational Security Document (OSD). Guidance for configuring audit logs will be provided in the OSD. Finally, the network administrator should coordinate with the OSC to establish procedures for reviewing logs on a weekly basis.

   Update: Several changes have been implemented. OCS has instituted an intrusion detection program where a managed security service provider (MSSP) monitors data captured in firewall logs. In addition, the application server audit feature has been enabled. Oracle database audit remains an issue – balancing performance against instituting a scaled down audit capability, based on the data sensitivity of the database.

2. Risk: Without monitoring, security violations or adverse trends may not be identified or addressed.

   Mitigation: EP&R/FEMA must develop and implement an effective life cycle process that includes design and security reviews, configuration management, and change control.

   Update: OCS is in the process of instituting an incident response program based on DHS guidelines, which has been forwarded to EP&R FEMA and DHS officials for review.

4. Risk: Without a management control process, there is no assurance that controls are implemented properly or consistently.

Mitigation: EP&R/FEMA must develop and implement an effective life cycle process that includes design and security reviews, configuration management (CM), and change control and each system must follow it.

Update: EP&R/FEMA has an integrated CM process to supplement an OCS-led security patch management program.

5. Risk: Employees and contractors cannot be expected to follow security procedures, nor can they be held accountable for their actions, if they are not trained regarding the "how" and "why" of info security. Security awareness and training are inadequate at the user, technical and managerial levels.

Mitigation: OCS is taking the lead to develop and implement an effective directorate wide information security training program. This includes developing and maintaining a training plan and guidance for maintaining training records, training materials and a training schedule. Based on this foundation, NFIRS program managers will have to include security training as part of new user orientation and ensure that its users participate in the overall training and awareness program. System specific security information is contained in the NFIRS OSD and should be used as the basis for all new user initial training. A plan will need to be developed to determine the most cost effective means for "back-training" current users.

Update: OCS is developing a security awareness and training program for the Enterprise using OPM guidelines (GoLearn.gov). System specific security features remain an area to be addressed.

6. Risk: Without separation of duties controls, one individual could have inappropriate access to system functions and data.

Update: This issue was mainly due to lack of separation of duties between the persons responsible for the development and production systems. Transfer of O&M responsibility is underway and anticipated to be completed by the end of July 2003.

**Low Risk**

1. Risk: Unattended workstations provide the opportunity for unauthorized people to gain access to systems and sensitive data. There is no logon banner to remind users of their responsibility to protect sensitive systems and data to provide a deterrent against unauthorized use.

Mitigation: Password-controlled screensavers should be implemented on all workstations. IT security training and awareness programs should emphasize the importance of not leaving workstations unattended and leaving workstations turned off when not in use. A logon banner is easy to implement and reminds users of their responsibility every time they log on. Such a banner can also be incorporated into an overall security awareness program by periodically including additional security reminders.

Update: OCS will address this enterprise problem through policy and other mechanisms including education and training. EP&R privacy and security policy statements are provided to Web users. Logon banners are used by EP&R/FEMA users, both LAN and remote access.

2. Risk: Sensitive data may be compromised, intentionally or inadvertently, if unauthorized personnel are able to view workstations that are in use. The NFIRS workstations are generally located within spaces that have controlled access.

Mitigation: Ensure unauthorized personnel are not able to view sensitive data displayed at a workstation. The NFIRS workstation at the disaster sites should be configured with password-protected screen savers and set for timeout after no more than three minutes. This configuration will provide some protection when the NFIRS disaster employee walks away from the workstation and minimize anyone from viewing EP&R/FEMA information. Additionally, users should be reminded to be aware of their surroundings and the potential for unauthorized/ inadvertent disclosure as part of the EP&R/FEMA security awareness program.

Update: Program office to manage this low risk deficiency. This Enterprise problem will be addressed through directorate policy and education and training.

3. Risk: The I&A risks found in this assessment were the result of poor implementation in privileged accounts (e.g., on servers) and include accounts without passwords, failure to meet length, complexity and aging requirements, and the use of hard coded passwords. Because of the access that such accounts provide, these risks should be addressed immediately. Traceability to an individual is not possible if group accounts or shared passwords are used.

Mitigation: Risks associated with I&A are easily mitigated by enforcing policies for all accounts. The most serious risk in this area, and the most difficult to remedy, is the use of hard coded passwords in the NFIRS software. The NFIRS program office has determined that the cost of rewriting code to provide individual accountability may be prohibitive in the short term. This issue may need to be addressed over time as NFIRS upgrades are developed and implemented. Remove hard coded user IDs from programs and applications

Update: Password strength requirements have been increased for web clients. Guest accounts have been disabled and privileged accounts minimized commensurate with operational requirements. The process accounts are required – the cost involved in re-engineering the application is deemed prohibitive by the program office; additional firewall protection have been installed to minimize risk. As indicated previously, the process accounts are still required – the cost involved in re-engineering the application is deemed prohibitive; additional firewall protection installed to minimize risk.

4. Risk: the Network Administrator does not perform Out-processing of employees, consultants, and contractors. If system accounts are not are not deleted from the system, the likely hood of an intruder access then system becomes greater, therefore, increasing the risk.

Mitigation: Have supervisors electronically submit and sign requests for creation and removal of user access. Requests are sent the Program Office for approval. As with the technical risks, operational risks can be mitigated through one-time changes to the system configuration, routine housekeeping activities, and adherence to published EP&R/FEMA standards.

Update: Program office will need to manage this low risk deficiency.

5. Risk: If a user ID and password are compromised without the user's knowledge, an unauthorized person could impersonate the authorized user.

Mitigation: After successful login, users must be given information reflecting the last login's time and date.

Update: Program office will need to manage this low risk deficiency – anticipate technical limitations on some of the operating systems may exist.

6. Risk: Inactive accounts provide an opportunity for an unauthorized user to gain system access.

Mitigation: System administrative personnel currently review inactive accounts every 90 days. Providing that resources are available, they should review inactive accounts every 30 days.

Update: Program office will need to manage this low risk deficiency.

7. Risk: NFIRS is not currently configured for 128-bit encryption, and cannot support high-end encryption.

Mitigation: Enable and configure 128-bit encryption for NFIRS secure web browser access.

Update: NFIRS will implement 128-bit symmetric encryption using SSL by the end of August 2003.

8. Risk: Inadvertent compromise could occur if media containing sensitive data are not properly controlled. Backup media is stored in fireproof safes but not stored off-site

Mitigation: NFIRS personnel should log deposits and withdrawals of backup tapes and other media and develop procedures for storing backup media in an OCS approved, off-site facility.

Update: Program office will need to manage this low risk deficiency. Capability addressed in updated contingency plan where restoration capability has been tested.

**CONCLUSION**

OCS commends the NFIRS staff for significant actions taken to address deficiencies noted in the risk assessment, particularly the successful testing of the NFIRS contingency plan.

After examination of subsequent application of mitigations by NFIRS staff, OCS considers the overall security risk level as ***low***.

Because residual risk is considered low level, OCS recommends that the NFIRS program office examine remaining low level security risk findings and apply appropriate risk management approaches to address their resolution.

Please return a signed copy of the enclosed NFIRS Accreditation Assessment to OCS, Attention: Richard Steadman, Bldg 429, Mount Weather. Questions should be directed to Richard Steadman, telephone (540) 542-2376.

Enclosures
NFIRS Accreditation Assessment, July 2003 (proposed)
NFIRS Security Plan, June 5, 2003
NFIRS Contingency Plan, Disaster Recovery and System Backup, May 28, 2003
NFIRS Risk Assessment, June 2003

**National Fire Incident Reporting System (NFIRS)**
**Accreditation Assessment**
**July 2003**

Reference: EP&R CIO Memorandum, subject: National Fire Incident Reporting System Statement and Request for Accreditation, dated July 11, 2003.

Therefore, weighing the remaining risk against operational requirements, my assessment, as the Designated Approving Authority for NFIRS, is as follows: **<initial in one block>**

RW 1. I find that the risk resulting with this NFIRS Certification is at an *acceptable* level. Therefore, I accredit the NFIRS. This accreditation decision requires that the NFIRS Program Office assume responsibility for the continued evaluation of risk to the NFIRS Critical Infrastructure and the EP&R/FEMA mission. This level of risk must remain at an *acceptable* level throughout the NFIRS system lifecycle. The NFIRS Program Office in consultation with the EP&R/FEMA OCS must conduct periodic independent evaluations of NFIRS to ensure that NFIRS continues to meet the requirements put forth in public law, Executive Directives, Federal standards and agency policies.

☐ 2. I find that the risk resulting from this NFIRS Certification is at an *acceptable* level, however I require that the NFIRS Program Office in consultation with OCS and develop and deliver a Plan of Action &Milestones (POA&M) NLT _____. This POA&M must outline the resolution of the deficiencies addressed in the Risk Assessment Vulnerability Findings. Therefore, I recommend continued operation with an Interim Approval to Operate (IATO) and a POA&M.

☐ 3. I find that the risk resulting from this NFIRS Certification is at an *unacceptable* level and require the following action:

a. ☐ Immediate shutdown

b. ☐ Continued operation with POA&M and re-certify

c. ☐ Other: _____

Signed,

R Paulison Date: 7/28/03

Dave Paulison
Director
Preparedness Division
Emergency Preparedness and Response