

**ORDER**

U.S. DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION

EA 1370.54

Eastern Region  
Jamaica, New York

MAR 2 2004

**SUBJ: Management of the Internet Monitoring Function in the Eastern Region**

---

1. **PURPOSE.** This Order establishes regional policy, procedures and guidelines on Federal Aviation Administration (FAA) Eastern Region Internet Monitoring of FAA Eastern Region employees and FAA contractors.

2. **DISTRIBUTION.** This Order is distributed to Division and Staff Office Branch Managers and above: all Field Offices and Facilities.

3. **BACKGROUND.** The Flight Standards Division, AEA-200, is responsible for maintaining the Eastern Region internet access point (IAP). AEA-200 has installed monitoring software at this IAP which has the ability to capture, analyze and report on internet browser activity.

The Aviation and Information Services Division, AEA-60, is responsible for maintaining the connection between the AEA Regional Office and the FAA Agency Data Telecommunications Network (ADTN). All AEA Regional Office internet traffic not using the AEA-200 IAP, uses one of the other FAA IAPs housed and maintained at other FAA locations. Such traffic must pass through the ADTN connection. It is neither desirable nor practical to restrict all internet traffic to one IAP. However, to date there is no monitoring software in place to capture, analyze, and report on internet browser activity passing through the ADTN connection.

4. **EXISTING POLICY.** Existing agency policies that are already in place address inappropriate and unlawful behavior regarding web internet access. These policies are excerpted in Appendix 1. The monitoring tools this document addresses will help enforce these policies.

5. **DELEGATION OF AUTHORITY.** The Security & Hazardous Materials Division, AEA-700, derives its authority to conduct investigations from the Federal Aviation Act of 1958 and Title 5 USC 73, which pertains to security, suitability and clearances and is the authority for employee and applicant investigations. Investigative jurisdiction is exercised generally to conduct investigations for several purposes including assuring the highest possible standards of integrity and ethical conduct are maintained by agency employees and representatives and in all agency operations (*FAA Order 1600.20B Civil Aviation Security Investigations Handbook*). AEA-700 is often requested to conduct thorough investigations into misconduct by employees and contractors concerning misuse of government property (i.e. computers, internet access). In addition, the Security & Hazardous Materials Division, AEA-700, is also responsible for investigating complaints referred from the Accountability Board within 30 working days (*FAA order 1110.125 Accountability Board*). Accountability Board complaints include allegations of intimidating, hostile, or offensive work environment based on race, color, religion, gender, sexual orientation, national origin, age or disability, sexual harassment or misconduct of a sexual nature and related reprisal.

6. **PROCEDURES.** The monitoring software currently used to capture, analyze, and report on internet browser activity passing through the IAP maintained by AEA-200 will also be installed at the AEA-FAA connection maintained by AEA-60.

All requests for internet usage information will be made in writing to the Manager, Security & Hazardous Materials Division, AEA-700, from the Manager of the requesting Division or Staff Office using the appropriate Internet Use Request EA Form 1370-53(12-03). This form is presented in Appendix 2. Managers and Supervisors are not to request internet usage information from AEA-200, AEA-60, or any IT staff directly. Requests in connection with suspected access to sexually explicit websites must first be reported to the Accountability Board, in accordance with FAA Order 1110.125.

In order to properly investigate allegations concerning internet misuse, internet usage information will be retained as captured by AEA-200 and AEA-60 for a minimum of 90 days, or longer if specifically requested by AEA-700, per the appropriate Internet Monitoring Extended Time EA Form 1370-53-1(12-03). This form is presented in Appendix 3.

Internet usage information will be used to support investigations conducted by AEA-700. In addition, division/staff managers, in support of internal investigations, may also use internet usage data, provided that the manager requests the information from AEA-700 in writing.

Allegations involving access to child pornography, or any other criminal activity, will be referred by AEA-700 to the proper law enforcement agency for investigation and prosecution.

To maintain employee privacy and to ensure the integrity of evidence, access to internet usage information will be accessible to AEA-700 investigators via a dedicated workstation in the offices of the Security & Hazardous Materials Division. AEA-200 will coordinate with AEA-700 to ensure the workstation meets the technical specifications to be able to access the software and data. AEA-200 will provide technical assistance to AEA-700 when needed. AEA-200 will also be responsible for software maintenance, including obtaining newer versions of the software when needed, and installing any necessary patches. To ensure that AEA-700 investigators can readily obtain any and all available reports, AEA-700 will coordinate with AEA-200 and AEA-60.



Arlene B. Feldman  
Regional Administrator

## APPENDIX 1

### FAA ORDER 1370.79A, INTERNET USE POLICY ABSTRACTS

According to *FAA Order 1370.79A, Internet Use Policy*, FAA Internet resources shall be used within prescribed mandates, laws and restrictions to improve information dissemination and to support business transactions. FAA Internet resources shall be used for valid work requirements and for limited personal use, provided such use does not:

- Interfere with FAA computer or networking services
- Burden FAA with additional incremental cost
- Interfere with an FAA user's employment or other obligations to the government
- Reflect negatively on the FAA or its employees
- Violate any Federal or FAA rules, regulations or policies

According to *FAA Order 1370.79A Section 6(a)(2) Improper Use of FAA Internet resources* includes:

Using the Internet for any purpose that violates the law or FAA rules, regulations and policies

Concealing or misrepresenting user identity or affiliation in electronic messages

Accessing or altering source or destination addresses of e-mail

Interfering with the supervisory or accounting functions of computer resources, including attempts to obtain system privileges unless authorized by system owners

Propagating chain letters, broadcasting inappropriate or unsolicited messages to lists or individuals, and comparable resource-intensive unofficial activity

Using FAA Internet resources for any commercial purpose, for financial gain (Including gambling) or in support of outside individuals or entities

Seeking, viewing, transmitting, collecting or storing vulgar, abusive, discriminatory, obscene (including sexually explicit or pornographic materials) or harassing messages or material

Attempting to libel, slander, or harass other users

Posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement, closely related to the employee's area of expertise and appropriate office approvals have been obtained

Engaging in matters directed toward any unauthorized fundraising, lobbying or partisan political activities

- Interfering with legitimate Internet services of any authorized user
- Representing the agency in an official capacity when not authorized to do so

FAA users must be aware that they have no expectation of privacy while using a Government-provided access to the Internet. Employee Internet and electronic messaging activities may be subject to monitoring, recording, and periodic audits to ensure that the system is functioning properly and to protect against unauthorized use. (FAA Order 1370.79A 6(e)(1))

APPENDIX 2

INTERNET USE REQUEST FORM - for use by Division / Staff Office

The \_\_\_\_\_ Division/Staff Office has received allegations of inappropriate computer activity that have occurred within the division/staff office. The specific activity is use of the internet to access and display inappropriate material on a computer screen in the workplace.

A notification of this allegation was filed with the FAA's Accountability Board on \_\_\_\_\_.

One potential source of information required to aid us in further determining the validity of the alleged activity is a report of the internet sites accessed by the identified workstation.

Therefore, we request a report of all internet sites accessed by the workstation assigned the internet protocol (IP) address of \_\_\_\_\_ from \_\_\_\_\_ to \_\_\_\_\_.

Please provide this information to me by close of business, \_\_\_\_\_. Thank you for your cooperation.

Here is what we can identify about the alleged misuse:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

APPENDIX 3

INTERNET MONITORING EXTENDED TIME FORM - for use by AEA-700

AEA-700 has received allegations of inappropriate computer activity that have occurred within the division/staff office. The specific activity is use of the internet to access and display inappropriate material on a computer screen in the workplace.

One potential source of information required to aid us in further determining the validity of the alleged activity is a report of the internet sites accessed by the identified workstation.

Therefore:

- We request that logs for this workstation continue to be maintained from \_\_\_\_\_ to \_\_\_\_\_ in anticipation of future retrieval.

Please return this form to AEA-700, with one of the following items checked off, when this log maintenance extension has been implemented.

- We have extended the log maintenance as requested.
- We are unable to extend the log maintenance as requested due to:

---



---



---



---



---



---



---

Technician: \_\_\_\_\_