

governmentattic.org

"Rummaging in the government's attic"

Description of document: Federal Aviation Administration (FAA) After Action

Report on January 2023 Notice to Air Missions database

failure

Requested date: 20-January-2024

Release date: 05-September- 2024

Posted date: 16- September-2024

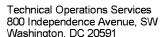
Source of document: National Freedom of Information Act Office, AFN-400

Federal Aviation Administration 800 Independence Avenue, SW

Washington, DC 20591 Fax: (202) 267-6514

Make an electronic request: Washington, DC FOIA

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.





September 5, 2024

This letter is in response to your Freedom of Information Act (FOIA) request, 2024-02031, dated January 20, 2024. Your request sought a copy of the Federal Aviation Administration After Action Report concerning the January 2023 Notice to Air Missions database failure.

A record search was conducted by the Air Traffic Organization and enclosed is the requested record. However, we are withholding portions of that record under FOIA exemptions 3 and 6.

FOIA Exemption 3 permits withholding of records specifically exempted from disclosure by another Federal statute. In this instance, 49 United States Code § 40119 states, in part, that the Department of Transportation (DOT) Secretary shall prescribe regulations prohibiting the disclosure of information that would be detrimental to transportation safety. These regulations may be found at 49 CFR part 1520, Sensitive Security Information. Specifically, 49 CFR § 1520.5(b) describes the types of records that may be withheld on the basis that they consist of Sensitive Security Information (SSI). The subject records, as described in 49 CFR § 1520.5(b)(13), include information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or Department of Homeland Security as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems. Specifically, we are withholding those portions of the record that identify file system names/directories, servers, and commands, as well as timelines for recovery that detail when specific technical actions were taken to restore the system.

FOIA Exemption 6 protects individuals against clearly unwarranted invasions of personal privacy. To be covered under FOIA Exemption 6, information must first meet a threshold requirement: it must fall within the category of "personnel and medical files and similar files." 5 U.S.C. § 552(b)(6). This is read broadly and includes all information that "applies to a particular individual." <u>U.S. dept. of State v. Washington Post Co.</u>, 456 U.S. 595, 602 (1982). Once that threshold is met, the focus turns to whether disclosure would "constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). When applying Exemption 6, agencies must determine whether there is a significant privacy interest in the requested information, evaluate the requester's public interest in disclosure, and balance those competing interests.

In this case, we are withholding the names of individuals and a cell phone number. With regard to such information, there is typically no public interest in disclosure, while there is at least some

privacy interest in keeping confidential these personal details. See, e.g., Smith v. dept. of Labor, 798 F. Supp. 2d 274, 283-85 (D.D.C. 2011). In addition, any information that does not directly reveal the operations of the federal government, the Supreme Court has stated, "falls outside the ambit of the public interest that the FOIA was enacted to serve." DOJ v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 775 (1989). After considering the extent to which disclosure of the above information would serve the public interest, we have determined that absent a justification to the contrary, any such interest is minimal when weighed against the personal privacy interests. As such, withholding is appropriate under FOIA Exemption 6.

If you owe fees for the processing of this request, an invoice containing the amount due and payment instructions will be enclosed with this letter.

The undersigned is responsible for this partial denial. You may request reconsideration of this determination by writing the Assistant Administrator for Finance and Management (AFN-1), Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC, 20591 or through electronic mail at: FOIA-Appeals@faa.gov. Your request for reconsideration must be made in writing within 90 days from the date of this letter and must include all information and arguments relied upon. Your letter must state that it is an appeal from the above-described denial of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA Appeal."

You also have the right to seek dispute resolution services from the FAA FOIA Public Liaison via phone (202-267-7799) or email (7-AWA-ARC-FOIA@faa.gov) noting FOIA Public Liaison in the Subject or the Office of Government Information Services (https://archives.gov/ogis) via phone (202-741-5770 / toll-free--1-877-684-6448; fax--202-741-5769); or email (ogis@nara.gov).

Sincerely,

James D. Linney

Deputy Vice President, Technical Operations Services

Enclosure

National Airspace System (NAS) Aeronautical Information Walka Petalent Enterprise System Service Outage Incident After-Action Report

Date: January 18, 2023



Prepared for and Presented to: Federal Aviation Administration

Point of Contact: (b) (6) NAS AS Program Manager Cell: (b) (6) (b) (6) (a) faa.gov

Spatial Front, Inc. 1568 Spring Hill Rd, Suite 300, McLean, VA 22102 | www.spatialfront.com Contract Number: DTFAWA-11-A-00185

This document is prepared for use by the Government and may contain proprietary methodology and techniques. This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed to the extent identified within the contract terms. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in all the pages of this submission.



Change History Log

Version	Description	Author	Date
1.0	Initial Draft	(b) (6)	1/18/2023
1.1	Final Report	(b) (6) (b) (6)	1/18/2023



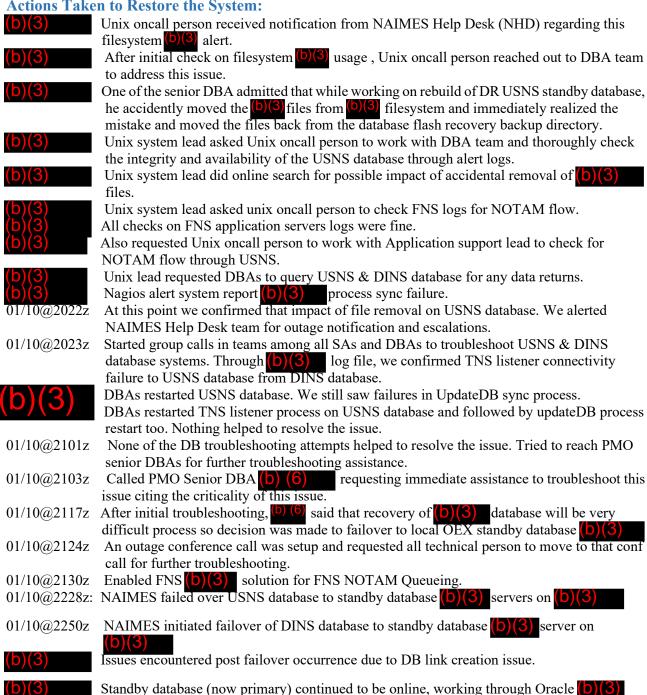
Overview

errors

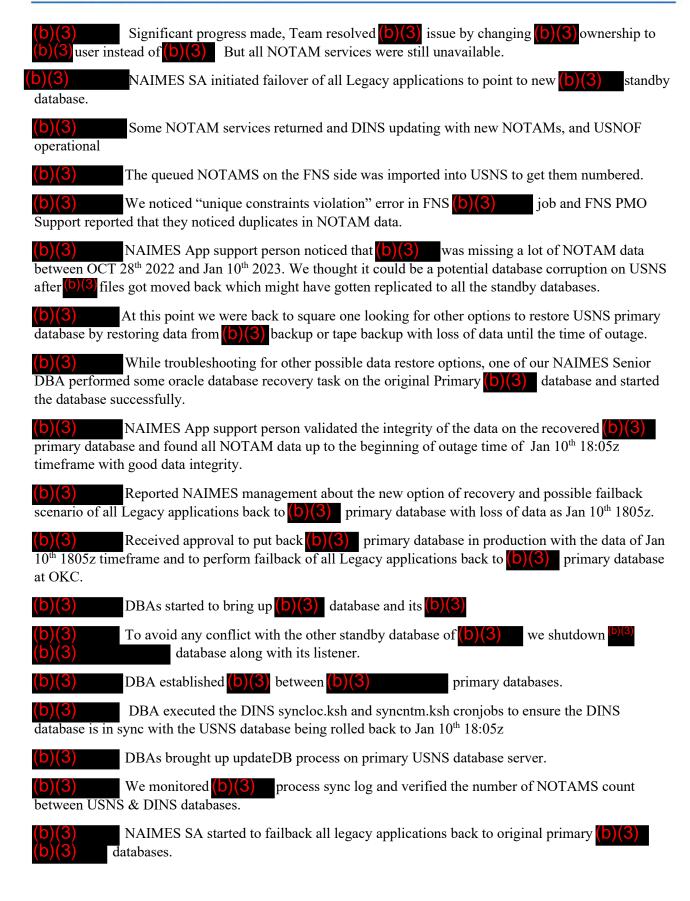
On 01/10/2023 @1819z: NAIMES Technical support team received critical Nagios alert reporting that the USNS database file system (b)(3) usage is full and reached 100%.

Timeline: 1819 UTC January 10, 2023

Actions	Taken	to	Restore	the	System:











Incident Reported: 1819 UTC January 10th, 2023 **Services Restored:** 1038 UTC January 11th, 2023

users.

Note: Post recovery a high system load was being observed as a result of increased utilization for FNS applications/services. A Return to Service post extensive monitoring and validation was provided at 01/15/2023 @ 2058z.



First NAS_AS Official Notified: (b) (6) — NAS infrastructure Team Lead

Root Cause:

It is clear from the log that the accidental deletion of (b)(3) files under (b)(3) on (b)(3) database initiated this outage. This outage could have been restored when we attempted to failover to standby USNS database at Oklahoma. We completed the failover successfully, but we found a lot of NOTAMs data missing which extended this outage time period to the next morning, leading up to the grounding of all flights.

Upon thorough troubleshooting and analysis of all events, we found that both the USNS and DINS databases were not syncing to any of the standby databases either at Oklahoma City or at Atlantic City datacenters. This out of sync situation on all standby databases caused the major impact on NOTAM systems.

Solution:

With the assistance from PMO senior DBAs, we successfully rebuilt all 3 standbys of USNS and DINS databases and synced them with the Primary.

Preventive Action:

- 1. We enabled 24/7 monitoring for all database syncs between primary and standby database servers with email notifications to all SA,DBAs, NAIMES Leads and NAIMES Help Desk team. Established a new process for the NAIMES Help Desk to create a ticket whenever they notice any mismatch of records in the sync alert. In this way, all sync issues will be addressed through our normal NAIMES problem ticket management process.
- 2. To avoid further accidental removal of critical files or any critical files in production systems, a buddy system is in place to watch over the shoulder of the engineer with another set of eyes to double check the commands and syntax executed.
- 3. We are researching a way to create a custom (b)(3) command with a provision of temporary recycle bin option just like windows for unix operating system In this way, we can restore system quickly from these recycle bins. This task is a work in progress and needs to go through proper testing in the lower environment before it is implemented.
- 4. Also, we are planning to report the status of all our database syncs between primary and standbys in our weekly Wednesday Operations Review meeting.

Lessons Learned:

The lack of continuous monitoring on (b)(3) between primary and standby servers caused the extended outage. We believe the databases went out of sync starting from the time of our disaster recovery simulation test back in October 28th 2022. We have to enhance our monitoring systems to catch any major critical events in the production system. It is a continuous process and we will continue to add more Nagios checks in place to avoid these kinds of outages in the future.