



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.S. dept. of State v. Washington Post Co., 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. Repts. 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 Management Enterprise System Service Outage Incident After-Action Report (NAIMES)

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) @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

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:

(b)(3) Unix oncall person received notification from NAIMES Help Desk (NHD) regarding this filesystem (b)(3) alert.

(b)(3) After initial check on filesystem (b)(3) usage, Unix oncall person reached out to DBA team to address this issue.

(b)(3) One of the senior DBA admitted that while working on rebuild of DR USNS standby database, he accidentally moved the (b)(3) files from (b)(3) filesystem and immediately realized the mistake and moved the files back from the database flash recovery backup directory.

(b)(3) Unix system lead asked Unix oncall person to work with DBA team and thoroughly check the integrity and availability of the USNS database through alert logs.

(b)(3) Unix system lead did online search for possible impact of accidental removal of (b)(3) files.

(b)(3) Unix system lead asked unix oncall person to check FNS logs for NOTAM flow. All checks on FNS application servers logs were fine.

(b)(3) Also requested Unix oncall person to work with Application support lead to check for NOTAM flow through USNS.

(b)(3) Unix lead requested DBAs to query USNS & DINS database for any data returns.

(b)(3) Nagios alert system report (b)(3) process sync failure.

01/10@2022z At this point we confirmed that impact of file removal on USNS database. We alerted NAIMES Help Desk team for outage notification and escalations.

01/10@2023z Started group calls in teams among all SAs and DBAs to troubleshoot USNS & DINS database systems. Through (b)(3) log file, we confirmed TNS listener connectivity failure to USNS database from DINS database.

(b)(3) DBAs restarted USNS database. We still saw failures in UpdateDB sync process. DBAs restarted TNS listener process on USNS database and followed by updateDB process restart too. Nothing helped to resolve the issue.

01/10@2101z None of the DB troubleshooting attempts helped to resolve the issue. Tried to reach PMO senior DBAs for further troubleshooting assistance.

01/10@2103z Called PMO Senior DBA (b)(6) requesting immediate assistance to troubleshoot this issue citing the criticality of this issue.

01/10@2117z After initial troubleshooting, (b)(6) said that recovery of (b)(3) database will be very difficult process so decision was made to failover to local OEX standby database (b)(3)

01/10@2124z An outage conference call was setup and requested all technical person to move to that conf call for further troubleshooting.

01/10@2130z Enabled FNS (b)(3) solution for FNS NOTAM Queueing.

01/10@2228z: NAIMES failed over USNS database to standby database (b)(3) servers on (b)(3)

01/10@2250z NAIMES initiated failover of DINS database to standby database (b)(3) server on (b)(3)

(b)(3) Issues encountered post failover occurrence due to DB link creation issue.

(b)(3) Standby database (now primary) continued to be online, working through Oracle (b)(3) errors

(b)(3) Significant progress made, Team resolved (b)(3) issue by changing (b)(3) ownership to (b)(3) user instead of (b)(3). But all NOTAM services were still unavailable.

(b)(3) NAIMES SA initiated failover of all Legacy applications to point to new (b)(3) standby database.

(b)(3) Some NOTAM services returned and DINS updating with new NOTAMs, and USNOF operational

(b)(3) The queued NOTAMS on the FNS side was imported into USNS to get them numbered.

(b)(3) We noticed “unique constraints violation” error in FNS (b)(3) job and FNS PMO Support reported that they noticed duplicates in NOTAM data.

(b)(3) NAIMES App support person noticed that (b)(3) was missing a lot of NOTAM data between OCT 28th 2022 and Jan 10th 2023. We thought it could be a potential database corruption on USNS after (b)(3) files got moved back which might have gotten replicated to all the standby databases.

(b)(3) At this point we were back to square one looking for other options to restore USNS primary database by restoring data from (b)(3) backup or tape backup with loss of data until the time of outage.

(b)(3) While troubleshooting for other possible data restore options, one of our NAIMES Senior DBA performed some oracle database recovery task on the original Primary (b)(3) database and started the database successfully.

(b)(3) NAIMES App support person validated the integrity of the data on the recovered (b)(3) primary database and found all NOTAM data up to the beginning of outage time of Jan 10th 18:05z timeframe with good data integrity.

(b)(3) Reported NAIMES management about the new option of recovery and possible failback scenario of all Legacy applications back to (b)(3) primary database with loss of data as Jan 10th 18:05z.

(b)(3) Received approval to put back (b)(3) primary database in production with the data of Jan 10th 18:05z timeframe and to perform failback of all Legacy applications back to (b)(3) primary database at OKC.

(b)(3) DBAs started to bring up (b)(3) database and its (b)(3)

(b)(3) To avoid any conflict with the other standby database of (b)(3) we shutdown (b)(3) (b)(3) database along with its listener.

(b)(3) DBA established (b)(3) between (b)(3) primary databases.

(b)(3) DBA executed the DINS syncloc.ksh and syncntm.ksh cronjobs to ensure the DINS database is in sync with the USNS database being rolled back to Jan 10th 18:05z

(b)(3) DBAs brought up updateDB process on primary USNS database server.

(b)(3) We monitored (b)(3) process sync log and verified the number of NOTAMS count between USNS & DINS databases.

(b)(3) NAIMES SA started to failback all legacy applications back to original primary (b)(3) (b)(3) databases.

(b)(3) USNS database online, USNOF operational through BHIV tool. Then we continued to bring up AISR & other Legacy NOTAM retrieval applications.

(b)(3) We brought up eRIDS and Oasis xml applications. With this we completed failback of all legacy applications. We then started to focus on FNS applications.

(b)(3) First we brought up (b)(3) Job on the FNS side to make sure FNS can pull all the USNS NOTAMS without any duplications as it occurred in our previous failover attempt. Job came up and successfully pulled all USNS NOTAMS without any duplication this time.

(b)(3) We noticed slowness in (b)(3) and at some time it runs fine but without any data refresh.

(b)(3) (b) (6) PMO wanted to change FNS queueing parameters to publish all unnumbered NOTAMS in FNS. After we made that change through (b)(3) portal and (b)(3) Job successfully refreshed data. But it was still slow at some time intermittently. It took almost hours to complete for few iterations. PMO FNS team suspected heavy volume of NOTAM data flow from USNS could be the reason for this slowness.

(b)(3) We successfully brought up all the FNS applications.

(b)(3) NOTAM systems available, data validation being performed - (USNS Stable)

(b)(3) NOTAM systems available, delay in FNS application/service response observed - (USNS Stable)

(b)(3) FNS delay continues, to free up additional resources on other FNS systems, NS application taken offline - (USNS Stable)

(b)(3) FNS delay continues, NAIMES/SLE degraded some apps/services to potentially reduce the high system load - (USNS Stable)

(b)(3) FNS delay continues, NAIMES/SLE occasionally stopping some FNS apps/services to improve performance - (USNS Stable)

(b)(3) FNS delay continues, Continuous troubleshooting efforts are in progress and no significant updates - (USNS Stable)

(b)(3) FNS delay continues, same status and troubleshooting efforts continue

(b)(3) FNS delay continues, same status and troubleshooting efforts continue

(b)(3) Started addressing data discrepancies between USNS/DINS with FNS and downstream users.

Incident Reported: 1819 UTC January 10th, 2023

Services Restored: 1038 UTC January 11th, 2023

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 (b)(3) 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.