Description of document:	Federal Aviation Administration (FAA) records re: change in policy regarding public releasability of En Route Intelligence Tool (ERIT) [radar] data, 2005-2010
Requested date:	24-April-2010
Appeal date:	26-August-2011
Released date:	11-January-2011
Material released on appeal:	01-September-2011
Posted date:	22-August-2011
Update posted:	19-September-2011
Date/date range of documents:	02-December-2005 – 08-December-2010
Source of document:	FOIA Coordinator Federal Aviation Administration National Freedom of Information Act Staff, ARC-40 800 Independence Avenue, SW Washington, DC 20591 Fax: (202) 493-5032 Online FOIA request form: Washington, DC FOIA
Note:	Additional material released on appeal follows material previously posted.

U.S. Department
of Transportation
**Federal Aviation
Administration**

Mission Support Services
800 Independence Ave., SW.
Washington, DC 20591

JAN 11 2011

This responds to your Freedom of Information Act (FOIA 2010-004656) request dated April 24. Your request sought a copy of all records that discussed the change in policy regarding En Route Intelligence Tool (ERIT) and/or why ERIT data can no longer be released to the public.

A records search was conducted in the FAA Mission Support Services Litigation Liaison Office. Enclosed are 49 pages responsive to your request. However, all personal telephone numbers have been redacted. This information has been redacted and is being withheld from disclosure under 5 U.S.C. 552 (b)(6). Exemption 6 of FOIA protects information that pertains to an individual "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Also, the information pertaining to radar antenna sites on memorandum dated December 8, 2010, has been redacted as it is non responsive to your request.

There are no fees associated with this request.

The undersigned is responsible for this partial denial. You may request reconsideration of this determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC, 20591. Your request must be made in writing within 30 days from the date of receipt of this letter and must include all information and arguments relied upon. Your letter must also 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 mark "FOIA."

Sincerely,

Carol Might
for
Elizabeth L. Ray
Vice President, Mission Support Services
Air Traffic Organization

Enclosures

Federal Aviation Administration

Memorandum

Date: December 8, 2010

To: Deanna Hall, Acting Manager, Management Support Team, ESC
Gail Kasson, Manager, Administrative Services Group, CSC
Johnathon Calkins, Team Manager, Management Support Team, WSC

From: Carol Might, Director, Litigation Liaison Office, Mission Support Services

Subject: Guidance for FOIAs Seeking Location of Radar Antenna Sites and Radar Data

Radar Antenna Sites

[redacted]

Radar Data

Fundamentally, FOIA requests for radar data are processed just like any other request. The responsible facility is required to search and retrieve the responsive records, then the facility's quality assurance (QA) office, in conjunction with the facility's Technical Operations office, must review the records and redact that which is sensitive. However, if the sensitive data cannot be reasonably segregated from that which is not sensitive, then the responsive record must be withheld in its entirety.

The guidance for responding to requests for raw radar data, such as ERIT, remains the same. We will not release raw radar. There was also some recent confusion as to whether CDR data can be released, because Order 6191.2, STARS System Security Handbook, classifies CDR data as SSI. However, according to Appendix E of 6191.2, the parts of the CDR data that are **not** SSI are target, tracking and flight plan data, which is the data we routinely release in FOIA and for discovery in litigation and enforcement cases.

In summary, the facility's QA office, in conjunction with the facility's Technical Operations office, have the technical expertise to review the responsive records and therefore must make the disclosure determinations for those FOIA requests that seek radar data, and then advise the Service Center FOIA office accordingly.

Please let me know if you have any questions or concerns with respect to the aforementioned guidance.

Attachment

[redacted]

Federal Aviation Administration

Memorandum

Date: DEC 2 2005

To: Acting Director, ATC Spectrum Engineering Services, Mailstop AJW-6

From: Director, Office of Internal Security and Investigations, AIN-1

Prepared by: Internal Security Policy Division, AIN-200

Subject: Sensitivity of United States Radar System Information

[redacted]

[redacted]

Re: Fw: ERIT data - feedback
Timothy S Wallace Dorothy Worden 03/02/2010 04:36 PM
AJR-22, Strategic Operations Security Group
Carol Might, Dean Torgerson

This message has been replied to.

Dottie & Carol,

The discussions I've had with Dean and Carol revolved around the following:

1) The hand-off beacon codes for normal air traffic fall within a prescribed range. Codes outside these ranges are used to designate special flights of national security interest (e.g., defense, law enforcement, etc.). Such knowledge could be used to determine which flights are operating with special status.

2) Knowing the hand-off locations and associated frequencies provide information on where frequency jamming or disruption operations could be conducted.

3) The two points above also form a mosaic argument; that the information above, combined with an air picture, could allow simplified reconstruction of choke points and vulnerabilities.

Did I miss anything Carol and Dean?
Tim Wallace, Security Planning Manager
System Operations Security (AJR-22)
Federal Aviation Administration
Air Traffic Organization
Email: timothy.s.wallace@faa.gov
SIPR: timothy.wallace@faa.csp.sgov.gov
[redacted]

"One Sky...Free and Secure"

WARNING: This correspondence may contain Sensitive Security Information and attachments that are controlled under 49 CFR 15 and 1520. No part of this correspondence may be disclosed to persons without a "need to know", as defined in CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C 552 and 49 CFR parts 15 and 1520.

Dorothy Worden I will probably need something along the lines of... 03/02/2010 04:22:36 PM

From: Dorothy Worden/AWA/FAA
AGC-400, Litigation/FOIA/Privacy Act
To: Carol Might/AWA/FAA@FAA
Cc: Dean Torgerson/AWA/FAA@FAA, Timothy S Wallace/AWA/FAA@FAA
Date: 03/02/2010 04:22 PM
Subject: Re: Fw: ERIT data - feedback

I will probably need something along the lines of what you all provided on ERIT. We need to beef up our arguments - especially when we had provided this information in the past.

Carol Might I agree. Tim, do you have any input? Dottie _ do... 03/02/2010 09:40:43 AM
Dorothy Worden/AWA/FAA

Dorothy Worden/AWA/FAA

AGC-400,
Litigation/FOIA/Privacy Act

03/02/2010 09:21 AM

To Carol Might/AWA/FAA@FAA, Dean Torgerson/AWA/FAA@FAA

cc

Subject Fw: ERIT data - feedback

Well, we got DOT legal concurrence.

On two FOIA appeals from Mr. Alan Smiley, we withheld hand off codes and beacon code ranges used by several FAA facilities, including the sector and frequencies for VFR and IFR and En Route, under Exemption 2. The denials were signed by the Southern Regional Administrator but the Eastern Service Center made the determinations. The rational is that the information requested could be used to mount a cyber attack on the NAS system.

Your thoughts?
----- Forwarded by Dorothy Worden/AWA/FAA on 03/02/2010 09:11 AM -----

From: <beth.kramer@dot.gov>

To: Dorothy Worden/AWA/FAA@FAA
Cc: <Bob.Ross@dot.gov>
Date: 02/26/2010 10:05 AM
Subject: RE: ERIT data - feedback

I am satisfied the data can't be redacted in any way to make parts releasable, without revealing security-sensitive information. My understanding of the explanation that Wayne Palaia provided below is:

While it's technically possible to filter the data to redact discrete, sensitive portions (e.g., portions showing VIP and entourage movements, military aircraft movements, and radar sensor locations - which are sensitive not only in real time but after-the-fact), it's just not possible to filter the data ENOUGH to ever completely eliminate the potential for ANY released portion of the data to reveal sensitive information.
For example:
(1) If enough partial data were released, the parts could be stitched together to make a complete/continuous air picture, that could then be used (in combination with a flight check test) to compute/identify gaps of radar sensor coverage (i.e., air space that's unmonitored, and air space that's less well monitored because of environmental conditions affecting sensor sensitivity).
[I think Wayne is saying that a FOIA requester could fly through air space, then request radar data for that date/time period, and figure out if there were areas where radar detection was less sensitive.]
(2) Any released portions could be combined/correlated with records of pilot radio traffic to identify security-sensitive air routes.

Beth
[redacted]iginal Message-----
From: Dorothy.Worden@faa.gov [mailto:Dorothy.Worden@faa.gov]
Sent: Thursday, February 25, 2010 8:45 AM
To: Kramer, Beth (OST)
Subject: Fw: ERIT data - feeback

Beth,

AGC-400,
Litigation/FOIA/Privacy Act

03/02/2010 09:21 AM

To Carol Might/AWA/FAA@FAA, Dean Torgerson/AWA/FAA@FAA
cc
Subject Fw: ERIT data - feedback

Well, we got DOT legal concurrence.

On two FOIA appeals from Mr. Alan Smiley, we withheld hand off codes and beacon code ranges used by several FAA facilities, including the sector and frequencies for VFR and IFR and En Route, under Exemption 2. The denials were signed by the Southern Regional Administrator but the Eastern Service Center made the determinations. The rational is that the information requested could be used to mount a cyber attack on the NAS system.

Your thoughts?
----- Forwarded by Dorothy Worden/AWA/FAA on 03/02/2010 09:11 AM -----

From: <beth.kramer@dot.gov>

To: Dorothy Worden/AWA/FAA@FAA
Cc: <Bob.Ross@dot.gov>
Date: 02/26/2010 10:05 AM
Subject: RE: ERIT data - feedback

I am satisfied the data can't be redacted in any way to make parts releasable, without revealing security-sensitive information. My understanding of the explanation that Wayne Palaia provided below is:

While it's technically possible to filter the data to redact discrete, sensitive portions (e.g., portions showing VIP and entourage movements, military aircraft movements, and radar sensor locations - which are sensitive not only in real time but after-the-fact), it's just not possible to filter the data ENOUGH to ever completely eliminate the potential for ANY released portion of the data to reveal sensitive information.
For example:
(1) If enough partial data were released, the parts could be stitched together to make a complete/continuous air picture, that could then be used (in combination with a flight check test) to compute/identify gaps of radar sensor coverage (i.e., air space that's unmonitored, and air space that's less well monitored because of environmental conditions affecting sensor sensitivity). [I think Wayne is saying that a FOIA requester could fly through air space, then request radar data for that date/time period, and figure out if there were areas where radar detection was less sensitive.]
(2) Any released portions could be combined/correlated with records of pilot radio traffic to identify security-sensitive air routes.

Beth
[redacted]
-----Original Message-----
From: Dorothy.Worden@faa.gov [mailto:Dorothy.Worden@faa.gov]
Sent: Thursday, February 25, 2010 8:45 AM
To: Kramer, Beth (OST)
Subject: Fw: ERIT data - feeback

Beth,

Here is additional support for withholding the ERIT data Do you concur or do you have additional concerns?

Dottie
----- Forwarded by Dorothy Worden/AWA/FAA on 02/25/2010 08:42 AM -----

From: Dean Torgerson/AWA/FAA
AJR-8, Litigation Office

To: Dorothy Worden/AWA/FAA@FAA

Cc: Carol Might/AWA/FAA@FAA

Date: 02/24/2010 11:55 AM

Subject: Fw: ERIT data - feeback

Dottie,

Below is the ERIT program office's response to my e-mail, which sought additional support for the argument that exempt data cannot be reasonably segregated from non-exempt data. In addition to that argument, Wayne also asserts in the last paragraph of his e-mail that the release of ERIT data shows gaps in radar coverage which will reflect surveillance vulnerability. Tim Wallace (System Operations Security) has expressed the same concerns, because those individuals with an intent to do harm can use the data to determine where they could operate undetected. Taking into account that the release of ERIT data exposes surveillance vulnerability, I would recommend that we uphold our denial.

Dean Torgerson
ATO FOIA Coordinator
ATO System Operations Litigation Support
[redacted]ed by Dean Torgerson/AWA/FAA on 02/24/2010 09:38 AM -----

Wayne
Palaia/ACT/FAA
AJW-146, ASR-9

To
Dean Torgerson/AWA/FAA@FAA

cc
Carol Might/AWA/FAA@FAA, Mark W Olsen/AWA/FAA@FAA

02/23/2010 06:24 PM

Subject
Re: ERIT data - feeback(Document link: Dean Torgerson)

Hi Dean -

Not knowing exactly what the argument "supports the position that the exempt (unfiltered data) data cannot be reasonably segregated from that data which is not exempt" ... there is not a document that provides details regarding "sensitive data".

Generally, in a conversation Tim Wallace spoke of a file containing 'items' that is required to be filtered ... I have no situational awareness on this file or the items desired to be filtered. Not seeing the file or discussing the specifics of each item to be filtered, at this time, I am unaware that Tech Ops has any such automated capability ... i.e., run utility application against each file. All filter actions would require manual data entry and validation. For instance, a 20MB file may for an ARTCC may contain target reports from numerous radar sites and many thousands of target reports (no weather data).

Is one engineer/technician dedicated for many hours "segregating" data items reasonable? ... you can easily substitute days for hours ... I cannot provide numeric qualifiable values because that is entirely dependant on skill set of operator, as well as, the effort depends on the quantity of data/files required and the quantity of items to be excluded, additionally, who validates all the "exempted" data is excluded?

I am going to understand "exempt (unfiltered data) data" to be VIP & entourage movements, military aircraft movements, surveillance radar sensor location (lat/long) ...

exact beacon codes may be identified in the application filter feature to include/exclude those specific target reports (beacon & reinforced) out of the resultant file ... this will not remove primary target reports

there is a possibility to include/exclude all target reports within a 'region' rendered on the computer display monitor defined by lat/long corners or drag a rectangle

site identifier (3 letter id) and sensor location (lat/long) may be 'stripped' from each file header

For a better understanding, the entire RDAS/ERIT activity is based on the theory of "analyzing" targets of opportunity as compared to "flight check" targets that originated in the late 1980s. The targets of opportunity "analysis" concept is that the performance of a particular surveillance radar sensor can be derived from the many thousands of target reports collected by implementing data reduction algorithms. The more data, the more accurate your metrics are expected to be, i.e., statistical analysis/approximation. The Radar Data Analysis (RDAS) activity and algorithms are a data reduction or summary reporting by "categorizing" each target report based on predetermined criteria/thresholds, i.e., probability of detection, false target analysis, collimation, blip scan, etc.

I am going to understand "data which is not exempt" to be non-sensitive general target reports ... if enough data (target reports) is available in the released data file:

one could still compute the surveillance radar coverage volume ... this could be displayed visually as a sphere or cylinder

if one or more adjacent (overlapping) radar sensors are included ... one could compute the 'gaps' of coverage, i.e., under, over, between

data files could be 'stitched' together to render a continuous 'air picture'

seasonal fluctuations in sensor sensitivity induced by temperature and environmental changes, i.e., bird migration, trees lose leaves, etc., may be identified and exploited

aircraft mishaps may be able to be identified ... afterall, FAA uses

RDAS/ERIT Data for search & rescue activities
air routes may be identified ... possibly correlated to AT-pilot radio traffic

Possibly scenario. A FOIA Requester can fly an aircraft through the requested airspace as a cooperative target (beacon/reinforced target) and/or an uncooperative target (primary/search only target) in predetermined 'flight patterns' with or without test and data recording equipment on board recording aircraft positional data. With the RDAS/ERIT released data, one could compute the performance and detection sensitivity of the surveillance radar sensor(s). The FAA refers to such planned and scheduled flight activities as a "flight check" test.

In summary, from an operational security (OPSEC) perspective, should any RDAS/ERIT Data files be released, one could identify the 'unmonitored' air space volumes and the surveillance perimeter that would be considered an air defense/air superiority vulnerability. The more surveillance radar data one could accumulate, regardless of how recent it was collected, would contribute to improve the identification accuracy of surveillance vulnerability(s) which cannot be 'filtered' out. The OPSEC persistence of the surveillance radar data does not diminish with time because ground based radar sites do not move.

I hope this provides enough technical details to support your argument.

thanx,
-wp

If you have questions about ERIT, please contact the AJW-146 Helpdesk - ERIT Support (609-485-7270)
--or-- 9-act-erit-support@faa.gov --or-- ERIT website Support Request webform.

Wayne Palaia
ERIT Engineering Team, AJW-146
FAA William J Hughes Technical Center
ATO-W, Building 270
Atlantic City Int'l Airport, NJ 08405
[redacted]

** PROPRIETARY & CONFIDENTIAL ** This email and any attachments are confidential and/or proprietary and intended solely for the named recipients. Unauthorized use, copying, or distribution is prohibited. If you received this e-mail in error, please notify me by replying and delete the message without copying or disclosing it. Thank you.

From:	Dean Torgerson/AWA/FAA AJR-8, Litigation Office
To:	Wayne Palaia/ACT/FAA@FAA
Cc:	Carol Might/AWA/FAA@FAA
Date:	02/23/2010 03:44 PM
Subject:	Re: ERIT data - feeback

Wayne,

As described in the email string below, the FAA has denied a request for ERIT data under exemption 2 (high), but the requester has appealed that denial. The FAA attorney and DOT attorney, who are reviewing the appeal, would like to see some more documentation that supports the position that the exempt (unfiltered data) data cannot be reasonably segregated from that data which is not exempt. In other words, we are looking for information which asserts that ERIT data cannot be reasonably filtered.

Thank you for your help. Please let me know if you have any questions.

Dean Torgerson
ATO FOIA Coordinator
ATO System Operations Litigation Support
[redacted]

Carol
Might/AWA/FAA

02/23/2010 10:41
AM

To
Dorothy Worden/AWA/FAA@FAA, Dean Torgerson/AWA/FAA@FAA

cc

Subject
Re: ERIT data - feeback(Document link: Dean Torgerson)

We can get more from the program office.
Dean - see if Wayne can help up.
Carol Might
Director, System Operations Litigation Support
[redacted]

----- Original Message -----
From: Dorothy Worden
Sent: 02/23/2010 10:39 AM EST
To: Carol Might
Subject: Fw: ERIT data - feeback

I forwarded your memo on ERIT and see below the DOT attorney's comments.
----- Forwarded by Dorothy Worden/AWA/FAA on 02/23/2010 10:38 AM -----

From: <beth.kramer@dot.gov>

To: Dorothy Worden/AWA/FAA@FAA

Date: 02/18/2010 05:58 PM

Subject: FW: ERIT data - feeback

Dorothy,
Based on what the FOIA Guide & cases in the Guide indicate, and reading the Program Office's descriptions as a complete stranger to the situation (like a Judge would), I don't feel persuaded yet! The Program Office needs to beef up the descriptions of burden and non-feasibility, before I would be on-board with the conclusion that the exempt & nonexempt info in the raw data are not "reasonably segregable." See my notes in red on the attachment.

Beth

-----Original Message-----
From: Dorothy.Worden@faa.gov [mailto:Dorothy.Worden@faa.gov]
Sent: Thursday, February 18, 2010 11:20 AM
To: Kramer, Beth (OST)
Subject: Fw: ERIT data

Hi Beth,

We have a FOIA appeal for ERIT data. The Program Office's position is that it is not releasable under Exemption high 2.

Before I draft the appeal response, can you look at the memo and see if you concur in their assessment? The memo was prepared by an FAA attorney.

Thanks.

Dottie
----- Forwarded by Dorothy Worden/AWA/FAA on 02/18/2010 11:15 AM -----

From: Carol Might/AWA/FAA

AJR-8, Litigation Office

To: Dorothy Worden/AWA/FAA

Cc: Melanie Yohe/AWA/FAA, Dean Torgerson/AWA/FAA, Jim Morin/AWA/FAA

Date: 12/08/2009 02:34 PM

Subject: Fw: ERIT data

See memo below. We knew we would face this eventually.

Carol A. Might
Director, System Operations Litigation Support
[redacted]

----- Forwarded by Carol Might/AWA/FAA on 12/08/2009 02:32 PM -----

To	Mark W Olsen/AWA/FAA AJS-7, Office of Risk Reduction Information	Carol Might/AWA/FAA@FAA
cc		
Subject	12/08/2009 01:52 PM	Fw: ERIT data

You owe me.

Mark

Mark W. Olsen
Federal Aviation Administration
Air Traffic Organization
Office of Safety

Manager, Search and Rescue
[redacted]
----- Forwarded by Mark W Olsen/AWA/FAA on 12/08/2009 01:51 PM -----

Carol
Might/AWA/FAA
AJR-8, Litigation
Office

10/07/2008 10:47
AM

To
Ken Myers/AWA/FAA@FAA, Douglas
Gould/AWA/FAA@FAA, Mark W
Olsen/AWA/FAA@FAA

cc

Subject
ERIT data

Gentlemen,

Attached is a memo - not to be shared - on my position for releasing ERIT data through FOIA. Basically we won't. I understand that Mark has issued a waiver to one person for search and rescue which I will need as I am heading up a new ATO wide FOIA training program.

Please read the memo and let me know if you see any problems and if it is technically accurate. Doug - it is a quick read, I know you can do it since it is based on National Security.

Thank you for your continued assistance.
(See attached file: ERIT Memo.doc)

Carol A. Might
Director, System Operations Litigation
[redacted]

[attachment "ERIT Memo.doc" deleted by Carol Might/AWA/FAA]

Federal Aviation Administration

Memorandum

Date: October 2, 2008

To: Carol Might, Director-System Operations Litigation

From: Holly Mullen

Subject: FOIA Requests for E-RIT Data

ISSUE: Is En Route Radar Intelligent Tool (E-RIT) data releasable under the Freedom of Information Act (FOIA)?

SHORT ANSWER: Ultimately, No. While E-RIT data, by definition, may be releaseable under the FOIA, an exemption to the statute [a 'high 2" analysis, as discussed in detail herein, focusing on the threat to homeland security], will apply in virtually all cases. Due to the inability to redact the actual "raw radar" itself, or, in the alternative, the unreasonable resources which would be required to review and redact tens of thousands of pages of text files of even a small portion of that data, the E-RIT data would be rendered unreleaseable.

BACKGROUND

The System Operations Litigation office recently received an inquiry as to whether E-RIT radar data should be released under the FOIA. According to the Regional FOIA POC's, FOIA requests for E-RIT radar data were received and fulfilled in the past. An alert employee contacted this office, expressing concern that information related to national security could be inadvertently released in E-RIT radar data. While the FOIA statute was enacted in order to allow public access to agency information, it is incumbent upon that agency to exercise caution when dealing with sensitive material—especially in a time of war.

E-RIT Radar Data

The En Route Radar Intelligent Tool (E-RIT) is a computer-based radar data recorder, designed to provide operational multi-sensor air traffic control sites with computer-based radar data recording and analysis tools. E-RIT radar covers airspace well beyond the boundaries of the facility that is using it. It is common that E-RIT radar data will contain events that are completely unrelated to the facility in question, many of which are matters related to homeland security. For example, E-RIT data may contain information related to military intercept and escort operations, Air Defense Identification Zone (ADIZ) violations and scramble procedures, Presidential asset placement, military movement and sensitive assets, and Secret Service activity.

E-RIT data is "raw" radar data, in that it has not been certified or corrected. It is used as a source of information only in events such as search and rescue activities. Certified radar data, such as data from the National Track Analysis Program (NTAP), is the most reliable data available. In all cases where E-RIT data was requested, certified data was also available.

FOIA ANALYSIS

Is It a Record?

With the passage of the Electronic Freedom of Information Act Amendments of 1996, the FOIA defines the term record as "including any information that would be an agency record . . . when maintained by an agency in any format, including an electronic format." Records Disposal Act, 44 U.S.C. 3301 (2000). In this case, the E-RIT radar data is information that is maintained by the agency in a format that is readable by a software program. Additionally, the FOIA requests for this data requested the E-RIT radar data in its original format. As such, E-RIT radar data is a record.

Is It an Agency Record?

In *U.S. Department of Justice v. Tax Analysts*, the Supreme Court articulated a two-part test for determining an agency record. Agency records are records that are: (1) either created or obtained by an agency; and, (2) under agency control at the time of the FOIA request. *U.S. Dep't. of Justice v. Tax Analysts*, 492 U.S. 136, 144-45 (1989). In determining whether an agency has sufficient "control" over a record, four relevant factors must be considered: (1) the intent of the record's creator to retain or relinquish control over the record; (2) the ability of the agency to use and dispose of the record as it sees fit; (3) the extent to which agency personnel have read or relied upon the record; and, (4) the degree to which the record was integrated into the agency's record systems or files.

In the present case, the E-RIT radar data was created by the agency, with agency equipment. It is also apparent that the E-RIT data was under the agency's control at the time of the FOIA request, because: (1) the agency created the data and intended to retain control; (2) the agency has full ability to use or dispose of the data; (3) although agency personnel do not rely on this data, they choose not to do so because it is not the most reliable source of information, not because they lack control over the data; and, (4) the data was full integrated into the agency's record systems and files. Based upon the foregoing, it is clear that E-RIT radar data is an agency record.

Do Any Exemptions Apply?

Under the FOIA, any "agency record" can be made the subject of a FOIA request. *See* 5 U.S.C. § 552(a)(3)). That said, an agency record may be withheld, to the extent that its content is of such sensitivity that it falls within a FOIA exemption. *See* 5 U.S.C. § 552(b).

Exemption two of the FOIA, found at 5 USC § 552 (b)(2), has been interpreted by courts to create two categories of information: "low two" information and "high two" information. *See, e.g., Schiller v. NLRB*, 964 F.2d 1205, 1207 (D.C. Cir.1992). Low two information relates to internal matters of a relatively trivial nature, while high two information deals with more substantial internal matters, the disclosure of which would risk circumvention of a legal requirement.

In the present case, the high two exemption applies, because E-RIT radar data is substantial internal information about the movement of aircraft in the National Airspace System. Due to the sensitivity of these matters in relation to national security, the disclosure of information found in E-RIT radar data would risk circumvention of a legal requirement.

Since September 11, 2001, the application of exemption two to those FOIA requests for agency records that are not classified, but nonetheless highly sensitive in light of homeland security concerns—has been upheld in nearly all courts. *See, e.g., Gordon v. FBI*, 388 F. Supp. 2d 1028 (N.D. Cal. 2005) (*upholding the high two exemption to a FOIA request for a "no fly list." the court found that "[r]equiring the government to reveal whether a particular person is on the watch lists would enable criminal organizations to circumvent the purpose of the watch lists by determining in advance which of the members may be questioned"*). Federal agencies are routinely reminded that they have a duty to protect sensitive information pertaining to the critical infrastructure from security breaches. The E-RIT radar data in question may contain information related to military intercept and escort operations, Air Defense Identification Zone (ADIZ) violations and scramble procedures, Presidential asset placement, military movement and sensitive assets, and Secret Service activity. Disclosure of this data would risk circumvention of a variety of legal requirements relating to national security and aviation safety. For example, E-RIT data, when put together, could determine a route that could allow for non-radar flight across the United States. In contrast, the risk of revealing the radar floor and non-radar corridors is not present when releasing certified data (such as NTAPS data).

Can the Data Be Redacted?

The final consideration is whether the data falling under exemption two can be redacted, and the remaining data released, pursuant to the FOIA request. In this case, redaction does not appear to be a viable option. E-RIT data is captured in a file format called RS3. There are several programs in the agency that can read this data, and one known program in the commercial community. Even in the RS3 format, redaction of primary data would require an unreasonable amount of labor, and—even then—there would be no assurances that the sensitive information was completely "erased" from the data.

Most requests for E-RIT data would be requests to convert the data to a text file, which involves some labor, but can be accomplished. Unfortunately, the text printout itself would be extremely voluminous (averaging 20 mgs of data), and the redaction would involve an unreasonable amount of skilled labor and time.

CONCLUSION

Based upon the foregoing, E-RIT data is, ultimately, not releasable under the Freedom of Information Act, because it falls under the "high two" exemption to the act, found at 5 USC § 552 (b)(2).

Re: Fw: For your feedback FOIA Update RDAS/ERIT ROB
Melanie Yohe Tina Leal 02/25/2010 11:45 AM
ARC-040, Planning and FOIA Staff
Dean Torgerson

Hi Tina,

You're talking apples and oranges. MOAs will not exist between FAA and a FOIA requester. MOAs for ERIT are made with the agency's trusted partners. I know we have a requester who is trying to become a trusted partner, which is spinning the discussion off course.

Dean Torgerson Tina, We have been very clear in advising the se... 02/25/2010 07:13:05 AM

From:	Dean Torgerson/AWA/FAA AJR-8, Litigation Office
To:	Tina Leal/ANM/FAA@FAA
Date:	02/25/2010 07:13 AM
Subject:	Re: Fw: For your feedback FOIA Update RDAS/ERIT ROB

Tina,

We have been very clear in advising the service centers that we will not release ERIT data. At the FOIA Summit in Renton last August that point was conveyed to all the FOIA staff and it will be reiterated today during the FOIA telcon. Please note that even if we could filter out the"exempt data," we would still withhold the ERIT data because it shows gaps in radar coverage.

Dean Torgerson
ATO FOIA Coordinator
ATO System Operations Litigation Support
[redacted]
Tina Leal/ANM/FAA

Tina Leal/ANM/FAA AJV-W5, Administrative Services Group	To	Dean Torgerson/AWA/FAA@FAA
	cc	
02/24/2010 04:26 PM	Subject	Fw: For your feedback FOIA Update RDAS/ERIT ROB

Tina Louise Leal
Management Analyst
ATO, Western Service Center
Administrative Services Group, AJV-W5
1601 Lind Avenue
Renton, WA 98057-4056
[redacted]
----- Forwarded by Tina Leal/ANM/FAA on 02/24/2010 01:26 PM -----

From: Tina Leal/ANM/FAA

AJV-W5, Administrative Services Group
To: Wayne Palaia/ACT/FAA@FAA
Cc: Barbara January/ANM/FAA@FAA, Joan Benson/ANM/FAA@FAA
Date: 02/24/2010 01:25 PM
Subject: Fw: For your feedback FOIA Update RDAS/ERIT ROB

As I read the rules of behavior, you indicate that one making FAA requests should send it to a FOIA Coordinator. The real question I have is did HQ make a decision on allowing this kind of data to be released under FOIA? As you know, a request for filtered data would take hundreds if not thousands of dollars in fees to process because it would take a considerable amount of time to drill down the filter. Given that scenario, I do not feel that the Service Center FOIA staffs should be a part of this type of request for information until a more fine-tuned process can be sorted out..

The reality is that the there may be SSI in this data. Which also means a request for a MOA between the requester and FAA. Requesters should have to agree to rules of behavior for ERIT in their MOA....

Tina Louise Leal
Management Analyst
ATO, Western Service Center
Administrative Services Group, AJV-W5
1601 Lind Avenue
Renton, WA 98057-4056
[redacted]

----- Forwarded by Tina Leal/ANM/FAA on 02/24/2010 01:20 PM -----

From: Geneva Renz/ANM/FAA
AJV-W5, Administrative Services Group
To: Barbara January/ANM/FAA@FAA, Joan Benson/ANM/FAA@FAA, Tina Leal/ANM/FAA@FAA
Date: 02/24/2010 01:12 PM
Subject: Fw: For your feedback FOIA Update RDAS/ERIT ROB

FYI.....

Geneva Renz
Management and Program Analyst/FOIA Coordinator, AJV-W5
DOT/FAA/ATO, Western Service Area
Administrative Services, Management Support Team - FOIA
1601 Lind Avenue S.W.
Renton, WA 98057-4056
[redacted]
Email: 9-ATO-WSA-FOIA@faa.gov
Fax: 425-203-4134

----- Forwarded by Geneva Renz/ANM/FAA on 02/24/2010 01:12 PM -----

From: Wayne Palaia/ACT/FAA
AJW-146, ASR-9
To: Dean Torgerson/AWA/FAA@FAA, Carol Might/AWA/FAA@FAA, Geneva Renz/ANM/FAA@FAA, Kenneth Ashworth/ANM/FAA@FAA, Lynda M Parra/ASW/FAA@FAA, Paula Watson/ASO/FAA@FAA, Timothy McCurdy/AWA/FAA@FAA, Timothy S Wallace/AWA/FAA@FAA, Tom Conroy/AMC/FAA@FAA, Steve Conklin/AWA/FAA@FAA, 9-AAL-FOIA/AAL/FAA@FAA
Date: 02/19/2010 12:59 PM
Subject: For your feedback FOIA Update RDAS/ERIT ROB

Hi All,

1. Attached is the an update to the <DRAFT> RDAS/ERIT Rules of Behavior with FOIA Request process ... this is a draft ready to implement ... I am coordinating with the Lab to implement a digital authentication/signature version ... I am just awaiting reasonable time for USAF Alaska via NDP to [hopefully] provide a military "reference basis" that surveillance data is higher than SSI, otherwise 'act as if' and drive on.

   I would be interested your feedback / recommendations (as we experienced prior, my peer review team of me, myself and I is not without its internal disagreements ... but I always wins out!).

   Your attention may be focused on:

   - Page 7 - Policies and Procedures Reference
   - Page 18 - section 3.5 Freedom of Information Act (FOIA) Requests for RDAS/ERIT Data
     I have listed each service center to include AJR-8 but did not include personnel names ... I obtained a June 2009 AAL FOIA document.

   Let me know of your critiques.

[attachment "ERIT Rules of Behavior (rev 2010.02.19).pdf" deleted by Melanie Yohe/AWA/FAA]

2. Attached are my 2007 comments ("Draft 1200.22D comments (email).txt) to draft 1200.22D that may be beneficial in that definitions of "NAS Data" ... I have been attempting to affect this change for sometime now.

[attachment "Draft 1200.22D comments (email).txt" deleted by Melanie Yohe/AWA/FAA]

3. Attached are the present ERIT Operating Locations (OL) ... this does not include the "ERIT Data Center" prototype ... ERIT Network is a share folder (authorized users only) that maps shortcuts to each ERIT OL ... some locations, such ZLC, require more data channels than one chassis can provide so two are implemented.

[attachment "ERIT OLs (20100128).pdf" deleted by Melanie Yohe/AWA/FAA]

thanx,
-wp

If you have questions about ERIT, please contact the AJW-146 Helpdesk - ERIT Support (609-485-7270) --or-- 9-act-erit-support@faa.gov --or-- ERIT website Support Request webform.

Wayne Palaia
ERIT Engineering Team, AJW-146
FAA William J Hughes Technical Center
ATO-W, Building 270
Atlantic City Int'l Airport, NJ 08405
[redacted]

** PROPRIETARY & CONFIDENTIAL ** This email and any attachments are confidential and/or proprietary and intended solely for the named recipients. Unauthorized use, copying, or distribution is prohibited. If you received this e-mail in error, please notify me by replying and delete the message without copying or disclosing it. Thank you.

Requester Robert Powell called re non-release of ERIT data

Jean Clark Dean Torgerson 10/01/2009 12:24 PM
AJV-C5, Administrative Services Group

This message has been forwarded.

Good morning Dean,

[redacted] called in reference to FOIA Request 2009-006494 and why we withheld the ERIT data from ZHU. I explained to him that our guidance changed and we are no longer able to release the ERIT data. He wanted to know why, so I told him it was raw radar data. He informed me that the radar data from I90 (Houston TRACON) was NTAP and that is raw data as well, it is just grouped. I told him that is the guidance we have received and it is best for him to go through the appeals process, which he said he would. But he wants to talk to someone and he chose Michael O'Harra, ASW-2. Michael signed the letter.

Michael is agreeable to talk to [redacted], but he would like someone with radar knowledge to be with him. I discussed this with my manager and she feels that since your office provided the guidance that your office should contact [redacted]

The actual data from I90 is PPB data.

Here is the request - 2009 - 006494CS.pdf

and the response letter - 2009 006494 [redacted] Partial Denial Exemption High 2.doc

[redacted] number is [redacted] Please let me know if you are going to contact him, so I can let Michael know. And I can also let [redacted] know when someone will be contacting him.

thank you for your assistance,
Jean Clark
FOIA Specialist

FAA, ATO Central Service Center
Management Support Team, AJV-C5
[redacted]

Link to Central Service Center Website

Feedback to Central Service Center: 9-ATO-CSC/ASW/FAA

U.S. Department
of Transportation
Federal Aviation
Administration

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

Fort Worth, Texas 76193-0000

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

[redacted]

Dear [redacted]

Subject: Freedom of Information Act (FOIA)
Request Number 2009-006494

This is in response to your letter dated August 15, 2009, requesting copies of certain radar data for 0100Z to 0400Z on August 4, 2009, for six radar installations in the Texas and Louisiana area.

A search was conducted at the appropriate air traffic facilities within the Central Service Area. We are enclosing one CD-ROM with radar data from the Houston Terminal Radar Approach Control in Houston, Texas.

The Enroute Radar Intelligence Tool (ERIT) data was located at the Houston Air Route Traffic Control Center. This data is being withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace.

The fees associated with your request total $13.35 for the radar data.

Payment may be made by check or money order payable to the Federal Aviation Administration. Please include your FOIA number on the bottom left-hand corner of your check. Your payment should be mailed to:

FAA/ATO Central Service Center
ATTN: Lynda Parra, AJV-C52
2601 Meacham Blvd.
Fort Worth, TX 76137

You can also make payment electronically through Pay.gov. A link from our FOIA web page (www.faa.gov/foia/) will take you to a secure website where you can pay by e-check or credit card. When you access the website, you will be asked to provide FOIA Web Payment ID 337517, your FOIA number, requester's name, and amount due.

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described partial denial determination. You may request an administrative review of the partial denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591.

Your request must be in writing within 30 calendar days from the date of receipt of the partial denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a partial denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

Your request has been assigned FOIA Number 2009-006494. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Jean Clark, Administrative Services Group, ATO Central Service Center, at 817-222-4945.

Sincerely,

Teresa A. Bruner
Regional Administrator,
Southwest Region

Enclosure

cc: (w/o enclosure)
Houston TRACON
Houston ARTCC
Regions and Center Operations – Planning and Freedom of Information Act Staff, ARC-40

AJVC52:JClark:jc:x4945:09/16/2009:N:MGTSUP/FOIA/2009006494Powellpartialdenial.doc

[redacted]

Re: For your feedback FOIA Update RDAS/ERIT ROB

Steve Conklin to: Wayne Palaia 02/22/2010 01:23 PM

Cc: 9-AAL-FOIA, Carol Might, Dean Torgerson, Geneva Renz, Kenneth Ashworth, Lynda M Parra, Paula Watson, Timothy McCurdy, Timothy S Wallace, Tom Conroy

Wayne,

We did several briefings up in AK last week, no show stoppers came out of the briefings which is good news. We are going to send a memo to the USAF asking them to define the conditions that they will allow the radar data to be distributed electronically via ERIT.

v/r,

Steve Conklin
National Operations Liaison
ATO-W NAS Defense Programs Office
AJW-151

[redacted]

WARNING: This correspondence may contain Sensitive Security Information and attachments that are controlled under 49 CFR 15 and 1520. No part of this correspondence may be disclosed to persons without a "need to know", as defined in CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C 552 and 49 CFR parts 15 and 1520.
Wayne Palaia/ACT/FAA

[redacted]

Wayne Palaia/ACT/FAA
AJW-146, ASR-9

02/19/2010 03:58 PM

To	Dean Torgerson/AWA/FAA@FAA, Carol Might/AWA/FAA@FAA, Geneva Renz/ANM/FAA@FAA, Kenneth Ashworth/ANM/FAA@FAA, Lynda M Parra/ASW/FAA@FAA, Paula Watson/ASO/FAA@FAA, Timothy McCurdy/AWA/FAA@FAA, Timothy S Wallace/AWA/FAA@FAA, Tom Conroy/AMC/FAA@FAA, Steve Conklin/AWA/FAA@FAA, 9-AAL-FOIA/AAL/FAA@FAA
cc	
Subject	For your feedback FOIA Update RDAS/ERIT ROB

Hi All,

1. Attached is the an update to the <DRAFT> RDAS/ERIT Rules of Behavior with FOIA Request process ... this is a draft ready to implement ... I am coordinating with the Lab to implement a digital authentication/signature version ... I am just awaiting reasonable time for

USAF Alaska via NDP to [hopefully] provide a military "reference basis" that surveillance data is higher than SSI, otherwise 'act as if' and drive on.

I would be interested your feedback / recommendations (as we experienced prior, my peer review team of me, myself and I is not without its internal disagreements ... but I always wins out!).

Your attention may be focused on:

- Page 7 - Policies and Procedures Reference
- Page 18 - section 3.5 Freedom of Information Act (FOIA) Requests for RDAS/ERIT Data
  I have listed each service center to include AJR-8 but did not include personnel names ... I obtained a June 2009 AAL FOIA document.

Let me know of your critiques.

ERIT Rules of Behavior (rev 2010.02.19).pdf

2. Attached are my 2007 comments ("Draft 1200.22D comments (email).txt) to draft 1200.22D that may be beneficial in that definitions of "NAS Data" ... I have been attempting to affect this change for sometime now.

Draft 1200.22D comments (email).txt

3. Attached are the present ERIT Operating Locations (OL) ... this does not include the "ERIT Data Center" prototype ... ERIT Network is a share folder (authorized users only) that maps shortcuts to each ERIT OL ... some locations, such ZLC, require more data channels than one chassis can provide so two are implemented.

ERIT OLs (20100128).pdf

thanx,
-wp

If you have questions about ERIT, please contact the AJW-146 Helpdesk - ERIT Support (609-485-7270) --or-- 9-act-erit-support@faa.gov --or-- ERIT website Support Request webform.

Wayne Palaia
ERIT Engineering Team, AJW-146
FAA William J Hughes Technical Center
ATO-W, Building 270
Atlantic City Int'l Airport, NJ 08405
[redacted]

** PROPRIETARY & CONFIDENTIAL ** This email and any attachments are confidential and/or proprietary and intended solely for the named recipients. Unauthorized use, copying, or distribution is prohibited. If you received this e-mail in error, please notify me by replying and delete the message without copying or disclosing it. Thank you.

ato
AIR TRAFFIC ORGANIZATION

Radar Data Analysis
Enhanced Radar Intelligent Tool

RDAS/ERIT
RULES OF BEHAVIOR

for

RDAS/ERIT USERS

ROB Revision: 2010.01.19

Prepared by:

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

AIR TRAFFIC ORGANIZATION
TECHNICAL OPERATIONS RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE
NATIONAL AIRWAY SYSTEMS ENGINEERING ASR-9 / RDAS TEAM
FAA WILLIAM J HUGHES TECHNICAL CENTER, ATLANTIC CITY, NJ 08405

RDAS/ERIT ROB ACKNOWLEDGEMENT

RDAS/ERIT ROB ACKNOWLEGEMENT: Users that possess a business need to access RDAS/ERIT Data shall comply with the Rules of Behavior described in the following pages and be approved for a one year subscription to the RDAS/ERIT Network and be added as a member to an RDAS/ERIT Network access control list.

RDAS/ERIT RULES OF BEHAVIOR

1. Comply with your access privileges.
2. Be familiar with ERIT security requirements.
3. You are responsible for any RDAS/ERIT Data you may download, transmit, store, or handle.
4. Do not connect any unauthorized hardware to the RDAS/ERIT information system/resources without appropriate coordination.
5. Know who is responsible for information systems security.
6. Know Your Rights and Responsibilities.
7. Report Security Incidents and Events.

By signing this RDAS/ERIT Rules of Behavior page below, you certify that you have read the RDAS/ERIT Rules of Behavior and that you agree to comply with these rules for the RDAS/ERIT Program described in the following pages.

APPLICANT / REQUESTOR

Name:

Title:

Organization:

Routing Symbol:

Telephone (voice):

E-mail:

Gov't Project/Program:

Site(s) to access:

Justification (business need):

I certify that I have read this document and will comply with these Rules of Behavior for the RDAS/ERIT Program.

Printed Name	Signature	Date	Routing Symbol

COTR / SUPERVISOR / MANAGER

Name:

Title:

Organization:

Routing Symbol:

Telephone (voice):

E-mail:

I certify that above requestor will comply with these Rules of Behavior for the RDAS/ERIT Program.

Printed Name	Signature	Date	Routing Symbol

To obtain user access to the ERIT Network, complete and sign this form, return this signed page to the RDAS/ERIT Program Management & Support Office who will process your request and retain a copy to record that your signature has been received. You may retain a copy of this page for your records, and may keep the rest of the document as a reference.

RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE
ASR-9 / RDAS Team, AJW-146 Helpdesk - ERIT Support
FAA / William J Hughes Technical Center
AJW-146, Building 270, Atlantic City Int'l Airport, NJ 08405

AJW-146 Fax: 609.485.6488
E-mail: 9-act-erit-support@faa.gov

Table of Contents

RDAS/ERIT RULES OF BEHAVIOR 4
Introduction 4
Applicability 4
Purpose 4
Training 5
OPSEC Primer 5
Policies and Procedures Reference 7
Terms & Definitions 9
RESPONSIBILITIES 11
1. Comply with your access privileges. 11
1.1. Appropriate Use 11
1.2. Consent to Monitoring 11
1.3. RDAS/ERIT Users Privileges 12
1.4. RDAS/ERIT Program Management & Support Office Responsibilities 12
1.5. RDAS/ERIT Site Administrator Privileges 13
1.6. Circumventing Security Measures 13
1.7. Remote Access 13
1.8. Electronic Mail (E-Mail) 14
1.9. Software Copyright Licenses 14
1.10. Internet Usage 14
1.11. User Account Management 14
1.12. User Password Management 14
2. Be familiar with ERIT security requirements 15
2.1. Protecting RDAS/ERIT Security Controls 16
2.2. Noncompliance 16
3. You are responsible for any RDAS/ERIT Data you may download, transmit, store, or handle. 16
3.1. Persistence of OPSEC Sensitivity of RDAS/ERIT Data 17
3.2. RDAS/ERIT Data shared with others 17
3.3. Access, Use, and Storage of RDAS/ERIT Data on Non-Government systems 17
3.4. Distribution of RDAS/ERIT Data 18
3.5. Freedom of Information Act (FOIA) Requests for RDAS/ERIT Data 18
4. Do not connect any unauthorized hardware to the RDAS/ERIT information system/resources without appropriate coordination. 20
4.1. RDAS/ERIT Interconnections To Other Systems 20
4.2. Removable Media Usage 20
4.3. Telecommunication for RDAS/ERIT 21
5. Know who is responsible for information systems security. 21
6. Know Your Rights and Responsibilities. 21
7. Report Security Incidents and Events. 22
7.1. Who Do You Report To? 23
7.2. Reporting Security Weaknesses 24

RDAS/ERIT RULES OF BEHAVIOR

Introduction

It is the responsibility of each user to assure the confidentiality, integrity, and availability of Radar Data Analysis (RDAS) / Enhanced Radar Intelligent Tool (ERIT) information, and information systems.

The RDAS/ERIT Rules of Behavior (ROB) clearly delineate the responsibility and behavior expected of all individuals accessing the system/resources and handling RDAS/ERIT surveillance radar data/information. These rules are available to every user as part of the RDAS/ERIT Network Subscription process and at least on an annual basis. These are rules by which all RDAS/ERIT Users must abide when accessing and handling RDAS/ERIT surveillance radar data/information.

Rules of Behavior are part of a comprehensive program to provide complete information security. These rules are established to hold users accountable for their actions and hold users responsible for information security. Users need to understand that taking personal responsibility for the security of their system and the information it contains is an essential component of their job.

Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Developing and promulgating ROBs such as these are a common security practice, and are required under most methodologies for certifying or authorizing systems.

Applicability

These Rules extend to all Federal Aviation Administration (FAA) Air Traffic Organization (ATO) personnel and any other persons using RDAS/ERIT information system/resources or accessing FAA ATO systems under formally established agreements. This includes any FAA or Department of Transportation (DOT) employee, contractor, subcontractor, consultant, and other federally funded users. All users should be fully aware of, and abide by, FAA security policies as well as related Federal policy contained in the Privacy Act, and Freedom of Information Act.

Submit suggestions for improvements

Each user will adhere to the procedures contained in the Rules of Behavior. If users subject to these procedures have suggestions for improving security procedures, technical measures, or security controls, they should consult with the RDAS/ERIT Program Management & Support Office.

Purpose

The primary objective of this document is to prevent unauthorized or inadvertent disclosure of Operational Security (OPSEC) sensitive information or data at all times, including during transmission or while stored on desktop/mobile/network systems. Any and all information associated with surveillance target/status/performance data is considered "sensitive unclassified information", as defined in of FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI).*

Compliance with these rules is not optional

This document does not replace or add to existing policies and procedures. Instead, this document summarizes and supports the objectives of those directives by defining key rules and behaviors each user must observe while interacting with RDAS/ERIT information system/resources.

These rules fulfill the requirement under FAA Order 1370.82A, *Information Systems Security Program* for Rules of Behavior and this document was developed to meet the specific needs of the FAA Air Traffic Organization, address the requirements of National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) Security Control PL-4 and for RDAS/ERIT Information system/resources.

Compliance with these rules is not optional.

These rules shall also govern the actions of non-RDAS/ERIT User personnel given access to RDAS/ERIT information systems.

Training

In addition to annual FAA Security and Hazardous Materials Security Awareness Virtual initiative (ASHSAVI), all users must acknowledge the Rules of Behavior prior to being granted access to RDAS/ERIT information system/resources. These rules are distributed to each RDAS/ERIT User (government and support contract) as part of the RDAS/ERIT Network Subscription Request process to ensure that they are made aware of their responsibilities when accessing RDAS/ERIT Information system/resources.

OPSEC Primer

The information that is often used against us is not classified information; it is information that is openly available to anyone who knows where to look and what to ask.

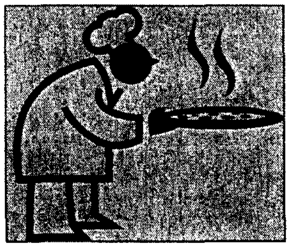
OPSEC Principles are something we see used everyday

Operations Security (OPSEC) is a tool that our adversaries believe in and one that we in the United States Government need to understand and integrate into our daily routine. What we do not always realize is how much we are giving away by our predictable behavior, casual conversations, routine acquisitions and other Internet information. Taking care of what we are revealing to those that are observing us will deny them the information pieces that may need to act in an adversarial way toward us.

What do people observe about your schedule? What do you do when you go to work? What are you revealing by your predictable routines and the way you do business; these are indicators. OPSEC helps us identify the indicators that are perhaps revealing information about missions, activities, and operations.

PIZZA STORY ... Desert Storm Scenario = *OPSEC INDICATORS*

- 400 Domino's Pizzas delivered to the Pentagon
- Numerous vehicles in Pentagon Parking Lots after duty hours



= **Start of Ground Invasion of Kuwait.**

What are OPSEC Indicators?

Who is observing at us? An adversary or competitor, such as a foreign intelligence service and corporate surveillance, that continues to collect information on us that may be used in the future for diplomatic reasons, for trade negotiations, as well as, security advantages in the case of terrorism. We sometimes only focus on what the most recent situation is but it is a certainty that those that would be our adversaries will continually look to find any weak links. Never underestimate the capabilities or strength of conviction of terrorists or any other adversary or competitor.

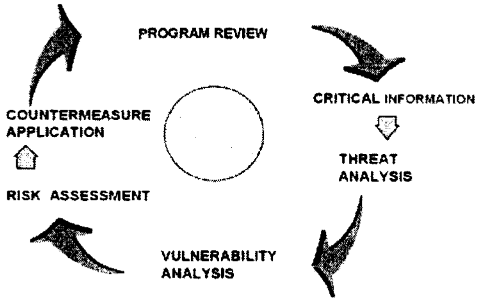
Consider the following sports example:

> OPSEC In Football ... The Play-action Pass Example:
>
> DESIGN - to Cause hesitation/delay action; freeze the linebackers and defensive backs, allowing receivers to gain an edge in getting open.
>
> DECEIVE - defensive linemen pursue a running back who does not have the ball.
>
> HIDE - the defense is unsure where the ball is, causing them to inappropriately commit focus and effort where it may not be needed.

Football teams protect their playbooks, disguise their plays, and guard their practice sessions. In short, they employ OPSEC to help ensure success.

OPSEC obviously is not the sole factor in being a successful football team; quality training, personnel, equipment, coaching, and strategy are all essential. OPSEC simply increases and enhances the opportunity for success.

THE OPSEC PROCESS:



Operations Security is a Five Step Process:

1. Identify Critical Information (CI)
2. Analyze the threat to the CI
3. Determine OPSEC vulnerabilities
4. Analyze and assess level of risk that can be tolerated
5. Implement appropriate countermeasures

OPSEC deals primarily with protecting (normally unclassified) information and indicators about our mission, capabilities and operations to help improve our chances for success.

Critical Information vs. Classified Information

Critical Information (CI) is identified because these 'bits of data' can potentially provide an adversary or competitor with knowledge of our intentions, capabilities or limitations. Each 'bit of data' can be classified, but classified information is normally protected through other more well-defined security regulations.

Information identified as CI is often not classified, but what the FAA refers to as sensitive unclassified information (SUI). (Reference FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)* and the FAA's Security and Hazardous Materials (ASH) Security Awareness Virtual Initiative (SAVI) annual training.)

Why not just classify the information? To be classified, information must meet strict criteria for which damage to national security can be clearly estimated and defined. When CI information is designated as sensitive unclassified information (SUI), it is not always known that a compromise of that information will positively cause damage to national security; however, it could cost us our technological edge, tip our hand to competitors, or jeopardize our people, resources, reputation and credibility.

You are the key to making OPSEC successful

CI Indicators are benign, subtle indicators or clues that point to CI. In order to protect CI, you must control, eliminate, or disguise the indicators.

Consider the real-world example of preparing for vacation: *Leaving your home unattended.*

> OPSEC On Vacation ...
>
> When most of us leave home for vacation, we take actions to protect our homes while we're away. We may:
>
> 1. Stop newspaper deliveries
> 2. Have the yard mowed
> 3. Buy light timers
> 4. Have a neighbor get the mail
> 5. In short, we want our houses to look like someone is home
>
> We protect our homes by using OPSEC principles. We could buy alarm systems, hire security guards, or use a house-sitter, but these options could be expensive and may not be cost-effective countermeasures considering the threat in our local area.

OPSEC employs (often low-cost) common sense methods to help protect the things that are most valuable to us.

CI Indicators are benign, subtle clues

OPSEC IS EVERYONE'S BUSINESS. Good OPSEC saves lives and resources; always use common sense and be aware.

OPSEC is a time-tested process that analyzes threats, identifies Critical Information, and develops appropriate countermeasures.

OPSEC is used by all of us in everyday life and is not so much a bunch of security rules, but a common-sense approach to viewing your operations through the adversary's or competitor's eyes.

OPSEC increases opportunities for mission success by protecting Critical Information.

Each of us are the key to making OPSEC successful!

Policies and Procedures Reference

The Rules of Behavior are consistent with the applicable laws, regulations, circulars, publications, orders, standards, handbooks, and documentation identified below:

- Public Law 100-235, *Computer Security Act of 1987*
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*
- Executive Order 13392, *Improving Agency Disclosure of Information*, dated December 14, 2005

- *The Freedom of Information Act*, as amended in 2002, 5 U.S.C. § 552
- Memorandum *The Freedom of Information Act (FOIA)* dated March 19, 2009, Office of US Attorney General
- Public Law 107347, Title III, *Federal Information Security Management Act (FISMA)* of 2002,
- Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005
- Office of Management and Budget (OMB) Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- The Privacy Act of 1974, as amended by The Computer Matching and Privacy Protection Act of 1988; 5 U.S.C. § 552a, and § 208 of the E-Government Act
- OMB, *Security of Federal Automated Information Resources*, Appendix III to OMB A-130 Circular, Management of Federal Information Resources, November 28, 2000
- Homeland Security Presidential Directive/HSPD-7, December 17, 2003
- DOT Order H 1350.2, *Information Systems Security Program*
- FAA Order 1200.22, *NAS Data and Interface Equipment Used By Outside Interests*
- FAA Order 1270.1, *Freedom of Information Act Program*
- FAA Order 1280.1B, *Protecting Personally Identifiable Information (PII)*
- FAA Notice 1370.42, *Password Administration In the FAA*
- FAA Order 1370.82A, *Information Systems Security Program*, September 11, 2006
- FAA Order 1370.97, *FAA Use of Non-FAA Workstations*, April 15, 2007
- FAA Order 1600.1D, *Personnel Security Program*
- FAA Order 1600.2D, *Security Classification Handbook*
- FAA Order 1600.6, *Physical Security Management Program*
- FAA Order 1600.66, *Telecommunications and Information Systems Security Policy*
- FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*
- FAA Order 6000.15D, *General Maintenance Handbook For National Airspace System (NAS) Facilities*
- ATO Order JO1370.11, *ATO Information Security Incident Reporting and Response Policy*

ATO Information Systems Security Program, FAA Orders reference:
https://intranet.faa.gov/faaemployees/org/linebusiness/ato/ato_issp/iss_review/FAA_orders/

Terms & Definitions

TERM — **DEFINITION**

RDAS/ERIT Information System/Resources

RDAS/ERIT Information System/Resources includes:

- data collection systems/devices (hardware & software)
- data repository/storage systems and media
- performance monitoring reporting displays and storage systems (hardware & software)
- network and data translation/transmission systems/devices (hardware & software)
- data decoding/data reduction/analysis algorithms, application tools, utilities
- documentation, user guides and technical references; and any resultant files, reports, printouts, graphics, and documents (digital/hardcopy)

duty to protect

Duty to protect means the recipient of the information has a duty imposed by law, regulation, or contractual agreement to protect the information from unauthorized access and disclosure.

need-to-know

Need-to-know is a fundamental security principle. It is a term given to the requirement that limits the flow (dissemination) of [sensitive] information only to those persons who require knowledge or possession thereof to perform authorized government functions or services. No person is entitled to knowledge or possession of classified information solely by virtue of his/her grade, office, or security clearance.

Responsibility for determining whether a person's duties require that he/she is authorized to receive it rests upon each individual who has possession, knowledge, or control of the information involved and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency, or a foreign government.

Critical Information (CI)

Critical Information (CI) is identified because these 'bits of data' can potentially provide an adversary or competitor with knowledge of our intentions, capabilities or limitations.

TERM **DEFINITION**

Operations Security (OPSEC)

Operations Security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified - concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC does not replace other security disciplines - it supplements them.

Our attention to security must change now. The events of September 11th, 2001 proved there is a demonstrated and known threat. How many times have we heard that terrorism is a threat? But, most of us thought it could only happen elsewhere - not in America. We are the representatives of the people. We develop, we plan, we execute - the American people trust us to do our jobs and keep them safe. The mishandling of information can put everything at risk and cost the lives of many Americans.

RDAS/ERIT Data

RDAS/ERIT Data is any unfiltered, unprocessed surveillance radar target/status/performance data content captured and collected from the communications lines, information system port or modem or equivalent is classified as *Sensitive Unclassified Information (SUI)*, "For Official Use only" (FOUO) and is **always** considered Operational Security (OPSEC) sensitive information that may be:

- displayed on your monitor screen/printer
- stored/shared in electronic format such as a file, database, printout, graphic
- held in storage or contained in transmission media
- retransmitted in another format
- or any other equivalent means

RDAS/ERIT Data Files

RDAS/ERIT Data Files contain:

- surveillance radar sensor positional, performance, status, coverage/volume information
- surveillance target position/tracking, status, performance information
- site adaptation information, site id, site parameters, example: the RS3 project file, RSDB (include mobileRSDB)
- any result output, graphical plot, tabular list, example: performance metric reports/files (digital/hardcopy)

Persistence of OPSEC Sensitivity

- Data regardless of how old/expired are considered Security Sensitive as they contain OPSEC sensitive information
- Data regardless of what medium it is stored on/in

RESPONSIBILITIES

1. Comply with your access privileges.

RDAS/ERIT Program Management & Support Office grants access to RDAS/ERIT information system/resources only to those who have a job-related need. Depending on your job responsibilities, you may have read-only access to the RDAS/ERIT Data/Network. If your manager or supervisor decides that you require changes to your RDAS/ERIT access privilege, you must follow established procedure for making the change and for coordinating with the RDAS/ERIT Program Management & Support Office.

1.1. APPROPRIATE USE

RDAS/ERIT hardware and software are for official government purposes. A user is authorized access to RDAS/ERIT information system/resources for official purposes only and will receive access only after completing the ERIT Network Subscription process. All activities not expressly permitted or prohibited, include, but are not limited to, the following:

PERSONAL USE, limited or otherwise, of RDAS/ERIT information system/resources is DISALLOWED.

- Taking information from RDAS/ERIT information system/resources for personal use, whether for profit, or any other purpose, or no purpose at all.
- Disclosing information about RDAS/ERIT information system/resources (or allowing it to be disclosed) to a nonuser without prior authorization.
- Tampering with another user's account, files, data or processes without the other user's express permission.
- Tampering or reverse engineering of RDAS/ERIT information system/resources.
- Using RDAS/ERIT information system/resources to store or develop personal information, such as address lists or data used in a personally-owned business, consulting business, or a second job.
- Use of RDAS/ERIT information system/resources communications features for political or other, non-business purposes, particularly any material any reader may find offensive.
- Using RDAS/ERIT information system/resources to record and store personal contact information for immediate family members, physicians, clergy, child or adult care providers, veterinarians, auto repair specialists, etc. Users are cautioned that personal information they record in message or word processing files are neither afforded nor eligible for privacy protection.
- No personal information will be downloaded to RDAS/ERIT information system/resources from any other system.
- RDAS/ERIT information system/resources will not be used for fraudulent, harassing or obscene messages and/or materials.

1.2. CONSENT TO MONITORING

Use of RDAS/ERIT information system/resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage are being observed.

1.3. RDAS/ERIT USERS PRIVILEGES

Regardless of the type of access you have, you should never try to access, view, modify, or delete parts of any system that you do not have authorization to access.

WHEN ACCESS IS NO LONGER REQUIRED to RDAS/ERIT information system/resources, notify the RDAS/ERIT Program Management & Support Office and make no further attempt to access these resources.

Submit suggestions for improvements

All RDAS/ERIT Users will adhere to the procedures contained in these Rules of Behavior. If users have suggestions for improving security procedures, technical measures, or security controls, they should consult with the RDAS/ERIT Program Management & Support Office.

All users needing access to RDAS/ERIT information system/resources are required to submit a completed RDAS/ERIT Network Subscription Request the RDAS/ERIT Program Management & Support Office and must have an active FAA Enterprise Network user account (Username). Authorized RDAS/ERIT Users will receive activation notification by e-mail that RDAS/ERIT Network privileges are appended and enabled to their Username account (by name).

If you have access beyond what you are supposed to have, you must notify the RDAS/ERIT Program Management & Support Office, and your supervisor immediately.

- RDAS/ERIT Users are authorized read-only privileges to RDAS/ERIT Data and the designated file/folder system that is "For Official Use Only" (FOUO) and OPSEC Sensitive.
- RDAS/ERIT Users are to access RDAS/ERIT information system/resources by authorized means only.
- RDAS/ERIT Data release outside the FAA requires additional coordination and authorization (reference this document section 3.2 *Distribution of RDAS/ERIT Data*).
- If your work position responsibilities change and you and your manager determine that the nature of your access to RDAS/ERIT information system/resources should change, you must notify the RDAS/ERIT Program Management & Support Office Help Desk (reference this document section 7.2 *Reporting Security Weaknesses*).
- Attempts to access any part of RDAS/ERIT information system/resources to which you have not been granted access, could cause result in loss of your RDAS/ERIT Data/Network access entirely and possibly FAA Enterprise Network.
- You are responsible for using Government-owned resources responsibly, in accordance with the requirements of your job, and for protecting these resources against unauthorized or disallowed use.

1.4. RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE RESPONSIBILITIES

The RDAS/ERIT Program Management & Support Office will perform all of the following prescribed duties as directed by the ERIT Standard Operating Procedures:

- The creation, modification, and deletion of user accounts and groups (local, built-in, remote)

- The assignment of user privileges based on the concepts of role-based access and least privilege
- The creation, modification, and deletion of file systems (folders); file system shares (folder)
- Audit log maintenance, to include log rotation, security alerts and activity logs, system inventory (applications, drivers, etc.)
- Maintain system configuration parameters and coordinate site adapted parameters
- As part of the annual SCAP, the RDAS/ERIT Program Management & Support Office submits audits reports and supports the security analysis

1.5. RDAS/ERIT SITE ADMINISTRATOR PRIVILEGES

RDAS/ERIT Site Administrators monitor system operation, report anomaly activity and perform on-site maintenance or modifications in coordination with the RDAS/ERIT Program Management & Support Office.

RDAS/ERIT Site Administrators assists the RDAS/ERIT Program Management & Support Office will administer the RDAS/ERIT security program at each ERIT Operating Location, as directed by FAA Order 1370.82A and the RDAS/ERIT Standard Operating Procedures.

RDAS/ERIT Site Administrators recommend to the RDAS/ERIT Program Management & Support Office interconnection to any other system and that such interfaces not be authorized or established; and, if currently in place, the interface will bc disconnected.

privileges granted to you are for the purpose of performing your work assignments

In addition, you must ensure that any elevated privileges granted to you for the purpose of performing your work assignments are not misapplied in order to gain access to information systems or to install unauthorized hardware or software. You occupy a position of trust and shall not erode the confidence placed in you by the FAA. Any evidence of such abuse may result in appropriate disciplinary action.

All RDAS/ERIT Site Administrators needing access to RDAS/ERIT information system/resources are required to submit a completed RDAS/ERIT Network Subscription Request the RDAS/ERIT Program Management & Support Office and submit a complete Coordination Worksheet. RDAS/ERIT information system/resource 'SysAdmin' privileges are appended to each RDAS/ERIT Site Administrator Username account (by name). ERIT Operating Locations may identify one or more RDAS/ERIT Site Administrators (backups/alternates).

1.6. CIRCUMVENTING SECURITY MEASURES

Except as directed by the RDAS/ERIT Program Management & Support Office for the purpose of testing and validating RDAS/ERIT information system/resource security controls, users will not attempt to circumvent any RDAS/ERIT procedural or technical measures used to protect the security of the system and the information it contains.

1.7. REMOTE ACCESS

Remote Access to the RDAS/ERIT information system/resources must be via authorized access methods. The current authorized access method to the Mission Support/Administrative networking environment is Virtual Private Network (VPN) issued by FAA Telecommunications Infrastructure Program (FTI/FRAC)

- Take precautions to secure government information and information resources.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Use only authorized licensed software on government equipment; do not violate Federal copyright laws.

- In accordance with FAA Order 1370.97 *FAA Use of Non-FAA Workstations*:
  - Adhere to all provisions or agreements related to off-site work.
  - Use virus protection software on off-site systems and keep it up-to-date.

Remote access users agree to protect the privacy and security of all ERIT data and equipment in the same manner as required when working at the office.

1.8. ELECTRONIC MAIL (E-MAIL)

User e-mail is not allowed, enabled, or supported on ERIT equipment.

1.9. SOFTWARE COPYRIGHT LICENSES

The RDAS/ERIT Program Management & Support Office is responsible for maintaining, obtaining, and procuring required licenses and informing users of license requirements. Specific questions regarding software copyright licenses will be addressed to the RDAS/ERIT Program Management & Support Office. Software not provided by the RDAS/ERIT Program Management & Support Office is prohibited on ERIT.

1.10. INTERNET USAGE

Access to and from the Internet from RDAS/ERIT information system/resources is limited only to direct business need such as technical information references to support ERIT hardware/software components.

Access to the Internet using ERAM support systems is authorized only through the FTI/FRAC remote access point and is restricted to only allow communications into RDAS/ERIT information system/resources through a Virtual Private Network connection using Government-Furnished Equipment.

1.11. USER ACCOUNT MANAGEMENT

Users must coordinate with their supervisor to create an account to access RDAS/ERIT information system/resources.

Password characteristics required for the RDAS/ERIT Network is consistent with FAA Enterprise Network strong password implementation.

Authorized users possessing privileges to RDAS/ERIT information system/resources are required to review and reauthorize all accounts on an annual basis. Inactive accounts, employee ascensions and separations (voluntary/involuntary) are identified and managed through the FAA Enterprise Network normal in-processing/out-processing.

1.12. USER PASSWORD MANAGEMENT

Password characteristics required for the RDAS/ERIT Network is consistent with FAA Enterprise Network strong password implementation. Always follow approved password management procedures.

Access to RDAS/ERIT information system/resources is password protected and any activity associated with your assigned Username account will be attributed to you.

Never divulge your password unless absolutely necessary

Regardless of the excuses given by another person for "needing" your password, never divulge your password unless absolutely necessary. Managers should not ask their employees for passwords, nor should system administrators. If an administrator needs to log in to your workstation or system for technical support activities, they should use an administrative login or should allow you to type your password. If a manager or system administrator must use your password, ask that the request be given to you in writing and signed by the requestor. In this case, or if you have the slightest reason to believe that your password has become compromised, intentionally or otherwise, change it immediately and report the event to the RDAS/ERIT Program Management & Support Office, or the ATO National Service Center (IT Help Desk) (reference this document "Report Security Incidents and Events" section).

If your password is compromised, change your password and report the circumstances under which the password was compromised to the RDAS/ERIT Program Management & Support Office, or the ATO National Service Center (IT Help Desk) (reference this document "*Report Security Incidents and Events*" section) immediately. This will help you prevent the compromise from happening again and may prevent damage to the FAA Enterprise Network and NAS.

Never record your password or Username in writing or electronically unless you take appropriate steps to safeguard the information by locking up written information or encrypting electronic data. If your password is initially given to you in writing, after you have logged in for the first time and subsequently changed the initial password, destroy the document that contains the password. "Destroy," means shredding or otherwise completely obliterating the information, since people who try to gain unauthorized access will often search through trash looking for such information.

There is also a danger posed by visitors in your work area, or even co-workers, who observe and record such information. Never assume that those around you do not know your habits or even your "secret" hiding place (such as taped under a drawer or keyboard).

Do Not Disclose Your Password To Anyone!

- Regardless of reason, do not share your password with anyone.
- Sharing your password with another person allows that person to utilize your user account using your Username (impersonating you).
- You are responsible and held accountable for all transactions associated with your Username.
- If your password is compromised, change your password and report the circumstances under which the password was compromised to the RDAS/ERIT Program Management & Support Office, or the ATO National Service Center (IT Help Desk) (reference this document "*Report Security Incidents and Events*" section) immediately.

2. Be familiar with ERIT security requirements.

If or when you are granted access to RDAS/ERIT information system/resources, you are responsible for helping to safeguard the system(s) you use and for being aware of the security requirements for the specific system resources you access.

2.1. PROTECTING RDAS/ERIT SECURITY CONTROLS

An RDAS/ERIT user may not divulge to non- RDAS/ERIT users specific information concerning RDAS/ERIT security equipment, software, or procedures in effect or proposed for adoption.

2.2. NONCOMPLIANCE

Users who do not comply with the prescribed RDAS/ERIT Rules of Behavior are subject to actions in accordance with existing policy and regulations, applicable union contracts or applicable Table of Penalties (contained in FAPM 2635, *Conduct and Discipline or Standards of Conduct* ER-4.1). These penalties include official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, and termination of employment. FAA will enforce the use of penalties against any user who willfully violates any FAA/ATO or Federal system security policy or order as appropriate.

3. You are responsible for any RDAS/ERIT Data you may download, transmit, store, or handle.

Each RDAS/ERIT Data electronic file is classified as "For Official Use Only" (FOUO) and shall be marked and handled as prescribed by FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI).* If you are unsure whether the data is sensitive, assume that it is, and safeguard it accordingly. Safeguards apply to printouts, to data showing on your screen, and to storage and transmission media. Devices for transmitting or storing data, such as disks, tapes, removable drives, etc., must also be safeguarded in accordance with the sensitive nature of the data or as FOUO which ever is higher.

RDAS/ERIT INFORMATION SYSTEM/RESOURCES includes data collection systems; data repository/storage systems; data translation/transmission systems; performance monitoring reporting displays, and database systems; data analysis algorithms, application tools, utilities; documentation, user guides and technical references; and any resultant files, reports, printouts and documents.

All RDAS/ERIT DATA is considered SECURITY SENSITIVE, "For Official Use Only" (FOUO) and is subject to FAA Order 1600.75 handling and marking and Order 1200.22 for distribution.

RDAS/ERIT DATA is any unfiltered, unprocessed surveillance target/status/performance data content captured and collected from the communications lines, information system port or modem or equivalent is ALWAYS considered Operational Security (OPSEC) sensitive information that may be:

- displayed on your monitor screen
- stored/shared in electronic format such as a file, database, printout, graphic
- held in storage or contained in transmission media
- retransmitted in another format
- or any other equivalent means

3.1. PERSISTENCE OF OPSEC SENSITIVITY OF RDAS/ERIT DATA

The persistence of OPSEC Sensitivity of RDAS/ERIT Data and the media is INDEFINITE and never expires regardless of age. No matter how old or expired RDAS/ERIT Data may be, surveillance sensor coverage/volume information may be computed in addition to possible air routes, etc.

ALWAYS handle and dispose of RDAS/ERIT Data appropriately in accordance with FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI).*

RDAS/ERIT DATA FILES contain

- surveillance radar sensor positional/coverage/volume information
- surveillance target/status/performance information
- site adaptation information, example: the RS3 project file
- any result output, example: performance metric reports (digital/hardcopy)

> * * RDAS/ERIT Data **PERSISTENCE OF OPSEC SENSITIVITY**, regardless of how old/expired, is considered Security Sensitive **INDEFINITE** as they contain OPSEC sensitive information and must be handled/disposed of appropriately (ref. FAA Order 1600.75).

3.2. RDAS/ERIT DATA SHARED WITH OTHERS

RDAS/ERIT Data may only be shared with other FAA employees who have a business or job-related need-to-know. FAA employees include government and support contract employees, transferring the responsibility to protect. This extends to data and any media that may contain data considered "expired" and "old" as they contain OPSEC sensitive information and must be handled appropriately.

ALWAYS sanitize media and dispose of RDAS/ERIT Data properly.

RDAS/ERIT systems are not certified

RDAS/ERIT Data cannot be used or substituted for a System Analysis Recording (SAR) or Continuous Data Recording (CDR). RDAS/ERIT Data collection systems, protocols and decoding/display tools/algorithms are not certified and cannot be used for any legal determinations. Each automation facility has certified systems to provide SAR/CDR data containing Air Traffic Control (ATC) information.

> RDAS/ERIT Data may only be shared with other FAA employees who have a business or job-related need-to-know.

3.3. ACCESS, USE, AND STORAGE OF RDAS/ERIT DATA ON NON-GOVERNMENT SYSTEMS

Access, use, and storage of RDAS/ERIT Data on Non- Government Systems must be authorized. These rules extend to Non-Government Systems that include but not limited to personal, home, and corporate information systems desktop/mobile/network equipment/devices, as well as, hardcopy and digital storage media equipment/devices.

- The user (government and contract support employee) has the 'duty to protect' the data and any media that may contain OPSEC sensitive information of any 'age' obtained from government sources in accordance with applicable policies and procedures (reference this document *Policies and Procedures Reference* section).

- The user (government and contract support employee) ALWAYS has the responsibility to handle and dispose of RDAS/ERIT Data specifically on Non-Government Information Systems appropriately in accordance with FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI).*
- The user (government and contract support employee) ALWAYS has the responsibility to report Security Incidents and Events of RDAS/ERIT Data specifically on Non-Government Information Systems appropriately in accordance with applicable policies and procedures (reference this document *Report Security Incidents and Events* section).

3.4. DISTRIBUTION OF RDAS/ERIT DATA

Distribution (sharing) of RDAS/ERIT Data to persons or organizations other than FAA must be authorized. This extends to data and any media that may contain data of any 'age' as they contain OPSEC sensitive information.

All RDAS/ERIT Data is "For Official Use Only", subject to compliance with FAA Order 1600.75 handling and marking, and requires compliance with FAA Order 1200.22, *NAS Data and Interface Equipment Used By Outside Interests* for RDAS/ERIT Data released outside the FAA to other U.S Government organizations/contractors.

The NAS Defense Program (NDP) serves as the FAA/ATO's coordination office for release or distribution guidance/authorization of RDAS/ERIT Data, reference FAA Order 1200.22, *NAS Data and Interface Equipment Used By Outside Interests.*

Forward requests to your service center or contact:

RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE

Call RDAS/ERIT Help Desk at: 609-485-7270
(staffed during normal business hours)
E-mail RDAS/ERIT Help Desk at: 9-act-erit-support.faa.gov

3.5. FREEDOM OF INFORMATION ACT (FOIA) REQUESTS FOR RDAS/ERIT DATA

All agencies of the United States government are required to disclose records upon receiving a written request unless the requested records are protected from disclosure by any of the nine exemptions or three exclusions of the FOIA enacted by the Congress to protect information that must be held in confidence for the Government to function effectively or for other purposes. This right of access is enforceable in court.

Why do I need to know about FOIA? You may be asked to assist in responding to a FOIA request for RDAS/ERIT Data. Individuals with the technical expertise regarding requested records are needed to identify where records may be found, and assist in making determinations on whether records should be released.

What should I do if someone asks me for FAA records? If you receive a telephonic or written request from an individual outside of the FAA for any FAA records, **forward ALL requests for RDAS/ERIT Data to the service center ATO FOIA coordinator**. All FOIA requests must be logged in the FOIA National Tracking System and assigned a FOIA tracking number.

Forward all FOIA Requests for RDAS/ERIT Data to your service center ATO FOIA coordinator.

The ATO FOIA coordinators for each service center are as follows:

EASTERN SERVICE CENTER

Administrative Services Group	AJV-E5

CENTRAL SERVICE CENTER

Administrative Services Group	AJV-C5

WESTERN SERVICE CENTER

Administrative Services Group	AJV-W5

ALASKA REGION

Flight Standards Division	AAL-200
E-mail:	9-AAL-FOIA.faa.gov

ATO SYSTEM OPERATIONS LITIGATION SUPPORT

ATO FOIA Coordinator	AJR-8

RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE

Call RDAS/ERIT Help Desk at:	609-485-7270 (staffed during normal business hours)
E-mail RDAS/ERIT Help Desk at:	9-act-erit-support.faa.gov

I'm really busy with my normal work---how much time do I have to respond to a FOIA?

When you are asked to assist with a FOIA response, the FOIA Coordinator will provide you with a suspense date and general instructions. Under the statute, federal agencies are generally required to respond to a FOIA request within twenty (20) business days, meaning that Saturdays, Sundays, and legal holidays are not counted. Some requests ask for expedited handling, meaning that the agency has ten business days to respond. The FOIA Coordinator will advise you if a request for expedited handling has been approved and revise the suspense date accordingly.

The requested RDAS/ERIT Data must be gathered and provided to the service center to be sequestered for final [legal] determination (potentially 6 or more years).

FOIA requests for RDAS/ERIT Data are time sensitive as per law.

Generally, when the FAA receives a FOIA Request for RDAS/ERIT Data, it will be assigned to the appropriate service area based on the ERIT Operating Location from which the data is sought. Each service center has an ATO FOIA coordinator (see above) who will contact the Air Traffic facility that hosts the data and coordinate gathering and storing the specific RDAS/ERIT Data files.

Typically, RDAS/ERIT Data is withheld under FOIA exemption 2 (high) and not released to the requester. It is important to note that even though the data will not be released to the requester, the Air Traffic facility must still 'pull' the requested RDAS/ERIT Data in the event that the requester appeals the FAA's determination for withholding the requested data. When we deny a FOIA request, we must keep the data for 6 years from date of the signed FOIA response letter. Should the requester appeal the FAA's determination the RDAS/ERIT Data must be maintained for 6 years after the appeal determination, or 3 years after final adjudication by courts, whichever is later.

4. Do not connect any unauthorized hardware to the RDAS/ERIT information system/resources without appropriate coordination.

Coordinate all configuration changes

There are many ways to change the RDAS/ERIT information system/resource configuration, including connecting another electronic device or computer, installing new hardware or software, downloading executable or self-launching files from the web and e-mail attachments, and so on. These changes can have unforeseen consequences for RDAS/ERIT information system/resources, "down stream" users and the FAA Enterprise Network systems/resources potentially enabling unauthorized access through ERIT (e.g., through a modem, IP port, etc.).

Coordinate configuration changes with the RDAS/ERIT Program Management & Support Office. The RDAS/ERIT Program is managed in accordance with FAA Configuration Management (CM) procedures (FAA Order 1800.66 *Configuration Management Policy*).

4.1. RDAS/ERIT INTERCONNECTIONS TO OTHER SYSTEMS

The RDAS/ERIT Program Management & Support Office will review the NAS Change Proposals and documentation regarding RDAS/ERIT information system/resource configuration and interconnections to other systems. The RDAS/ERIT Program Management & Support Office will verify that written Memorandums of Understanding (MOU) and/or Memorandums of Agreement (MOA) are developed jointly and authorizations are obtained between RDAS/ERIT information system/resource and the other system. The MOUs and/or MOAs will be approved prior to authorization of any interconnection to any other system.

Coordinate all interconnections to other systems, specifically NAS operational, to prevent security compromises

If the MOUs and/or MOAs do not exist, the RDAS/ERIT Site Administrator will recommend to the RDAS/ERIT Program Management & Support Office that such interfaces not be authorized or established; and, if currently in place, the interface will be disconnected.

A user may not connect RDAS/ERIT information system/resources to any other information system without prior authorization from the RDAS/ERIT Program Management & Support Office.

4.2. REMOVABLE MEDIA USAGE

Scan all removable media with up-to-date anti-virus software before inserting into your workstation computer or the RDAS/ERIT information system/resources. Removable media from unidentified sources may be infected with a virus that could be transmitted to RDAS/ERIT information system/resources and the FAA Enterprise Network.

> If you do not have virus protection software on your machine, contact the RDAS/ERIT Program Management & Support Office Help Desk immediately.

Ensure that all removable media is scanned for the presence of viruses

Contact the RDAS/ERIT Program Management & Support Office Help Desk immediately if you do not have anti-virus software on your machine. All users should implement virus protection software on all systems used to access, process and exchange RDAS/ERIT Data and RDAS/ERIT information system/resources.

4.3. TELECOMMUNICATION FOR RDAS/ERIT

The FAA Telecommuting Handbook addresses a supervisor's authority to permit specific persons to perform assigned duties outside the normal office setting. The directive stipulates that such arrangements meet all of the following criteria:

- Supervisors and employees must agree to the terms of the working arrangement and record the agreement in writing.
  - The agreement must identify the site(s) at which telecommuting work will be performed.
  - The agreement must contain telephone contact information.
  - The agreement must describe the telecommuter's work schedule.

5. Know who is responsible for information systems security.

YOU are ultimately responsible for the security of the RDAS/ERIT information system/resources you work with. Every FAA employee, contractor, guest, and system user has the same responsibility to safeguard the availability, integrity, and confidentiality of the data, and to be accountable for his or her actions.

** *UNDERSTAND YOUR INDIVIDUAL SECURITY RESPONSIBILITIES* **

- You should be familiar with, and practice, these Rules of Behavior
- You should know who to report actual or suspected violations (event or incident) to, and what constitutes suspicious activity
- You should also know how to keep up to date with FAA security directives, and RDAS/ERIT security implementations

6. Know Your Rights and Responsibilities.

FAA employees, contractors, and guests must be aware that they have no expectation of privacy when using any Government-provided resources, such as RDAS/ERIT information system/resources or when accessing the Internet or e-mail networks. All employee, contractor, and guest communications using Government facilities may be subject to monitoring, recording, and periodic audits to ensure that the system is functioning properly, to protect against unauthorized use, and to ensure that policies and regulations are being followed and enforced.

PERSONAL USE, limited or otherwise, of RDAS/ERIT information system/resources is DISALLOWED.

7. Report Security Incidents and Events.

Whether you are aware of an event or an incident, you must report it immediately in accordance with ATO Order JO1370.11, *ATO Information Security Incident Reporting and Response Policy* (para 8i, 8j and 8k).

You must report real or suspected information security events/incidents, immediately, to the National Operations Control Center (NOCC), or the ATO National Service Center (IT Help Desk).

When in doubt, report it!

In other words, if you have any reason to be believe that security has been, may be, or could be compromised; report it. No matter how unsure you are, report your suspicions, because what you know may fit with other pieces of information to help resolve an issue or avoid one. When in doubt, report it! Be prepared to describe the circumstances under which the event or an incident occurred, including the date and time, any people involved, and any other information that could help the system administrator mitigate the potential damage to the system.

What Do You Report? Anytime you see suspicious activity on your network, workstation or your server, you should report it. Suspicious activity is considered the act of a violation of an information system or network.

You should understand a "security event" and when it is considered a "security incident".

(Note: future tense)

Security Event = anything that has the potential for compromising Surveillance Radar Sensitive Data security or RDAS/ERIT information system/resources.

(Note: past tense)

Security Incident = if Surveillance Radar Sensitive Data security or RDAS/ERIT information system/resources have already been compromised.

You must report real or suspected information security events/incidents immediately to the NOCC or ATO NSC.

Reportable information security events/incidents:

- suspicious activity
- computer virus activity
- password lost or compromised
- PIN lost or compromised

Report any incidents of suspected fraud, waste or misuse of FAA systems to appropriate officials.

Report real or suspected Events / Incidents

- As a trusted user of RDAS/ERIT information system/resources it is your responsibility to report anything unusual.
- Make note of when and where the possible incident occurred. And keep note of the location, and be prepared to describe how you detected the incident.
- When you believe there has been an attempt to break into RDAS/ERIT information system/resources or any suspicious activity such as unauthorized access to RDAS/ERIT information system/resources, must be reported.

The types of widely recognized activities or violations are listed below to give you an idea of what to report. These activities or violations include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Social Engineering Attempts

<u>Why Should You Report Suspicious Activity</u>? By reporting suspicious activity, you can receive technical assistance; your reported activity may be associated with other incidents; your report supports incident statistics collection; contacting others raises security awareness; and reporting incidents is simply the responsible thing to do. Most importantly, your reporting of suspicious activity could play a major role in the protection of your own information.

7.1. WHO DO YOU REPORT TO?

You must report real or suspected information security events/incidents to the National Operations Control Center (NOCC), or the ATO National Service Center (IT Help Desk) and your Supervisor and/or Manager. The NOCC/NSC will coordinate with the appropriate entities, ATO NAS and Mission Support / Administrative Systems ISSM and the SIG as appropriate. ISSM/SIG will coordinate to obtain all pertinent security occurrence information, distribute information as needed for analysis, communicate with applicable FAA and Non-FAA entities, track status of the occurrence, direct any termination of services, and close the reported occurrence when resolved.

Report a real or suspected information security events/incidents **<u>for NAS systems</u>** contact:

1. Your Supervisor and/or Manager and your incident management chain, who should in turn contact the National Operations Control Center (NOCC).
2. If you are unable to contact anyone in your incident management chain, report the incident directly to the NOCC.

Call NOCC Operations Desk at:
703-904-4488

Report a real or suspected information security events/incidents **<u>for Administrative and Mission Support Systems</u>** contact:

1. Your Supervisor and/or Manager, System Administrator and your incident management chain or the RDAS/ERIT Program Management & Support Office help desk, who should in turn contact the ATO National Service Center (IT Help Desk).
2. If you are unable to contact any of the above, report the situation to the NSC.

Call NSC at:	866-954-4002
E-mail NSC at:	NSC@faa.gov

7.2. REPORTING SECURITY WEAKNESSES

RDAS/ERIT Users are obligated to report any discovered or noted technical or procedural security weaknesses as soon as possible, to the RDAS/ERIT Program Management & Support Office helpdesk.

Report a security weakness:

For RDAS/ERIT information system/resources contact:

RDAS/ERIT PROGRAM MANAGEMENT & SUPPORT OFFICE

Call RDAS/ERIT Help Desk at: 609-485-7270
(staffed during normal business hours)
E-mail RDAS/ERIT Help Desk at: 9-act-erit-support.faa.gov

ADDITIONAL MATERIAL RELEASED ON APPEAL

U.S. Department
of Transportation
**Federal Aviation
Administration**

Assistant Administrator for Regions
and Center Operations
800 Independence Ave., SW.
Washington, DC 20591

SEP 01 2011

RE: Freedom of Information Act Request 2010-003775R

This letter is in response to your correspondence dated August 26, 2011, submitted as a Freedom of Information Act (FOIA) administrative appeal to the Federal Aviation Administration (FAA). Your administrative appeal was remanded to this office for further processing, and has been assigned FOIA Control Number 2010-003775R.

In your initial FOIA request dated March 21, 2010, you asked for copies of all letters responding to FOIA requesters that deny access to radar data. In my initial response letter dated August 5, 2011, I provided you with five records responsive to your request. These records were provided to you in full, except that the names and addresses of the requesters were withheld under FOIA Exemption 6, which permits agencies to withhold information which if disclosed would constitute a clearly unwarranted invasion of personal privacy. In your FOIA Appeal dated August 6, 2011, you challenged this initial determination, and argued that the name as well as the city and state pertaining to each requester should be released.

Based on further review, it is clear that the name of FOIA requesters should be released, as this information is of such a nature that no expectation of privacy exists. See FOIA Update, Vol. VI, No. 1, at 6. However, it is also well settled that while there may be cases where the privacy interest of individual person(s) in their name may be non-existent, there is generally a stronger privacy interest in withholding other personally identifiable information such as phone numbers and home addresses which would trigger a balancing test involving the public benefit in disclosure against the individual right to privacy. See People for the Am. Way Found. v. Nat'l Park Serv., 503 F. Supp. 2d at 304, 306. In such cases, the analysis turns on the nature of the document and its relationship to the "core purpose" of the FOIA, which is to shed light on an agency's mission and the performance of its statutory duties. Information which does not directly reveal the operations of the federal government falls outside the ambit of the public interest that the FOIA was enacted to serve. In this case, the individuals in question clearly have a significant privacy interest in not having any part of their home address disclosed. Having found a significant privacy interest in this information, the public interest in disclosure was balanced against the privacy interests of the individuals involved. It is the responsibility of the requestor to identify the qualifying public interest in disclosure (a qualifying public interest is one that sheds light on an agency's performance of its statutory duties). Since you have asserted no qualifying public interest and since it is otherwise unclear how release of any part of the home address of the individuals involved would shed additional light on the FAA's performance of its statutory duties, the withholding of this information is proper under FOIA Exemption 6. However, as noted above, we are releasing to you the names of the five FOIA requesters.

The undersigned is responsible for this partial denial. You may request reconsideration of this determination by writing:

Assistant Administrator for Regions and Center Operations
Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

Your request for reconsideration must be made in writing within 30 days from the date of receipt 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."

Sincerely yours,

Douglas C. Taylor, PhD.
Director of Administration

Enclosure

U.S. Department
of Transportation
Federal Aviation Administration

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

2601 Meacham Blvd.
Fort Worth, TX 76137-000

JAN 22 2010

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

Mr. Gary P. Hart
[redacted]

Dear Mr. Hart:

Subject: Freedom of Information Act (FOIA)
Request Number 2010-001461

This is in response to your letter dated December 10, 2009, requesting central Missouri radar data from the Federal Aviation Administration (FAA) flight operations on November 30, 2009 and all active FAA air route traffic control antennas covering the Wheatland, Missouri, area.

We are enclosing antenna data for the Springfield-Branson Regional, Missouri, Airport Traffic Control Tower (ATCT). There are no fees associated with your request.

Regarding the request for radar returns and antenna heights, the records have been retrieved and reviewed. It has been determined that these records will be withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace.

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described partial denial determination. You may request an administrative review of the partial denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591.

Your request must be in writing within 30 calendar days from the date of receipt of the partial denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a partial denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

CONCURRENCES
ROUTING SYMBOL
MS JClark
JC
1-15-10
ROUTING SYMBOL
MSTeam GKasse
ROUTING SYMBOL
AJV-C5 [illegible]
ROUTING SYMBOL
AJV-C AKim
1/19/10
ROUTING SYMBOL
AJV-C KNezer
ROUTING SYMBOL
ASW-2
1/21/10
ROUTING SYMBOL
ASW-1
1/21/10

Your request has been assigned FOIA Number 2010-001461. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Jean Clark, Administrative Services Group, ATO Central Service Center, at 817-222-4945.

Sincerely,

Original Signed by
TERESA A. BRUNER

Teresa A. Bruner
Regional Administrator,
Southwest Region

Enclosure

cc: (w/o enclosure)
Kansas City ARTCC
Springfield, MO ATCT

AJV-C52:JClark:jc:x4945:01/15/2010:N:MGTSUP/FOIA/2010001461Hartpartialdenial.doc

U.S. Department
of Transportation
Federal Aviation
Administration

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

2601 Meacham Blvd.
Fort Worth, TX 76137-0000

[illegible]

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

Ms. Debbie Ziegelmeyer
[redacted]

Dear Ms. Ziegelmeyer:

Subject: Freedom of Information Act (FOIA)
Request Number 2010-001687

This is in response to your letter dated December 21, 2009, requesting radar data for the St. Louis, Missouri, area for December 15, 2009.

Regarding your request for radar returns, the records have been retrieved and reviewed. It has been determined that these records will be withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace.

There are no fees associated with your request.

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described denial determination. You may request an administrative review of the denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591.

Your request must be in writing within 30 calendar days from the date of receipt of the denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

Your request has been assigned FOIA Number 2010-001687. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Jean Clark, Administrative Services Group, ATO Central Service Center, at 817-222-4945.

Sincerely,

Teresa A. Bruner
Regional Administrator,
Southwest Region

cc: St. Louis TRACON

AJVC52:JClark:jc:x4945:01/15/2010:N:MGTSUP/FOIA/2010001687Ziegelmeyerdenial.doc

CONCURRENCES

ROUTING SYMBOL
MS/JClark
INITIALS/SIG
DATE

ROUTING SYMBOL
MSTeam /GKasson
INITIALS/SIG
DATE

ROUTING SYMBOL
AJV-C5/GNielsen
INITIALS/SIG
DATE

ROUTING SYMBOL
AJV-C/AKim
INITIALS/SIG
DATE

ROUTING SYMBOL
AJV-0/KNezer
INITIALS/SIG
DATE

ROUTING SYMBOL
ASW-2
INITIALS/SIG
DATE

ROUTING SYMBOL
ASW-1
INITIALS/SIG
DATE

ROUTING SYMBOL
INITIALS/SIG
DATE

U.S. Department of Transportation
Federal Aviation Administration

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

2601 Meacham Blvd.
Fort Worth, TX 76137-0000

SEP 1 9 2009

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

Mr. Robert M. Powell
[redacted]

Dear Mr. Powell:

Subject: Freedom of Information Act (FOIA)
Request Number 2009-006494

This is in response to your letter dated August 15, 2009, requesting copies of certain radar data for 0100Z to 0400Z on August 4, 2009, for six radar installations in the Texas and Louisiana area.

A search was conducted at the appropriate air traffic facilities within the Central Service Area. We are enclosing one CD-ROM with radar data from the Houston Terminal Radar Approach Control in Houston, Texas.

The Enroute Radar Intelligence Tool (ERIT) data was located at the Houston Air Route Traffic Control Center. This data is being withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace.

The fees associated with your request total $13.35 for the radar data.

Payment may be made by check or money order payable to the Federal Aviation Administration. Please include your FOIA number on the bottom left-hand corner of your check. Your payment should be mailed to:

FAA/ATO Central Service Center
ATTN: Lynda Parra, AJV-C52
2601 Meacham Blvd.
Fort Worth, TX 76137

You can also make payment electronically through Pay.gov. A link from our FOIA web page (www.faa.gov/foia/) will take you to a secure website where you can pay by e-check or credit card. When you access the website, you will be asked to provide FOIA Web Payment ID 337517, your FOIA number, requester's name, and amount due.

CONCURRENCES

ROUTING SYMBOL	INITIALS/SIG	DATE
MS/JClark		
MSTeam /GKa		
AJV-C5/GNiel		
AJV-C/AKim		
AJV-0/KNezer		
ASW-2		
ASW-1		

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described partial denial determination. You may request an administrative review of the partial denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591.

Your request must be in writing within 30 calendar days from the date of receipt of the partial denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a partial denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

Your request has been assigned FOIA Number 2009-006494. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Jean Clark, Administrative Services Group, ATO Central Service Center, at 817-222-4945.

Sincerely,

Original Signed By:
Michael C. O'Harra

Teresa A. Bruner
Regional Administrator,
Southwest Region

Enclosure

cc: (w/o enclosure)
Houston TRACON
Houston ARTCC
Regions and Center Operations – Planning and Freedom of Information Act Staff, ARC-40

AJVC52:JClark:jc:x4945:09/16/2009:N:MGTSUP/FOIA/2009006494Powellpartialdenial.doc

U.S. Department
of Transportation
**Federal Aviation
Administration**

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

2601 Meacham Blvd
Fort Worth, TX 76137

SEP 25 2009

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

Mr. Robert M. Powell
[redacted]

Dear Mr. Powell:

Subject: Freedom of Information Act (FOIA)
Request Number 2009-006761

This is in response to your letter dated September 2, 2009, requesting copies of certain radar data for 2300 Zulu on August 27, 2009, and 0330 Zulu on August 28, 2009, in the Kansas City, Missouri, area.

A search was conducted at the appropriate air traffic facilities within the Central Service Area. The En Route Radar Intelligence Tool (ERIT) data was located at the Kansas City Air Route Traffic Control Center. This data is being withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace.

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described denial determination. You may request an administrative review of the denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591.

Your request must be in writing within 30 calendar days from the date of receipt of the partial denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a partial denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

Your request has been assigned FOIA Number 2009-006761. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Lettie Perez, Administrative Services Group, ATO Central Service Center, at 817-222-5564.

Sincerely,

Original Signed by
TERESA A. BRUNER

Teresa A. Bruner
Regional Administrator,
Southwest Region

cc: Minneapolis Center/Kansas City Center/Kansas City Intl ATCT

AJVC52:LPerez:lp:x5564:09/21/2009:N:MGTSUP/FOIA/2009-6761 Powell denial exempt 2.doc

CONCURRENCES

ROUTING SYMBOL	INITIALS/SIG	DATE
AJV-C52/LPerez	lp	9/22/
AJV-C52/GKass	GKass	9/22/09
AJV-C5/GNielsen	Rcc	9/22/09
AJV-C/AKim	AKim	9/22/09
AJV-C/KNezer	Lcc	9/22/09
ASW-2		9/24/09
ASW-1	tab	9/24/09

U.S. Department
of Transportation
Federal Aviation
Administration

Southwest Region
Arkansas, Louisiana,
New Mexico, Oklahoma,
Texas

2601 Meacham Blvd
Fort Worth, TX 76137

CERTIFIED MAIL—RETURN RECEIPT REQUESTED

Mr. Robert M. Powell
[redacted]

Dear Mr. Powell:

Subject: Freedom of Information Act (FOIA)
Request Number 2009-006996

This is in response to your letter dated August 22, 2009, requesting copies of certain radar data for the time period of 0100 to 0400 Zulu on August 6, 2009, for various locations.

A search was conducted at the appropriate air traffic facilities within the Central Service Area. The En Route Radar Intelligence Tool (ERIT) data was located at the Houston Air Route Traffic Control Center. This data is being withheld from disclosure under Exemption 2 of the FOIA. Title 5 U.S.C. 552(b)(2) protects internal data, the disclosure of which would risk circumvention of a statute or agency regulations, or impede the effectiveness of an agency's activities. The data is considered critical infrastructure and the release of which could cause harm to the security of the national airspace. We are enclosing a CD-ROM containing radar data from the Houston Terminal Radar Approach Control. The fees associated with your request are $13.35 for the CD-ROM.

Mr. Konstantine Nezer, Jr., Director, ATO Central Service Center, and the undersigned are the officials responsible for the above described partial denial determination. You may request an administrative review of the denial determination by writing to the Assistant Administrator for Regions and Center Operations, Federal Aviation Administration National Headquarters, 800 Independence Avenue, SW, Washington, DC 20591. Your request must be in writing within 30 calendar days from the date of receipt of the partial denial determination, and must include all information and arguments relied upon. Your letter must state that it is an appeal from a partial denial determination of a request made under the FOIA. The envelope containing the appeal should be marked "FOIA."

Your request has been assigned FOIA Number 2009-006996. Please refer to that number in any further correspondence concerning this matter. If you have any questions regarding this request, you may call Lettie Perez, Administrative Services Group, ATO Central Service Center, at 817-222-5564.

Sincerely,

Original Signed By:
Michael C O'H[illegible]

Teresa A. Bruner
Regional Administrator,
Southwest Region

Enclosure
cc: Houston TRACON/Houston Center

AJVC52:LPerez:x5564:10/8/2009:N:MGTSUP/FOIA/2009-6996 Powell denial exemption highthe 2.doc

CONCURRENCES
ROUTING SYMBOL AJV-C52/LPerez
INITIALS/SIG LP
DATE 10/8/09
ROUTING SYMBOL AJV-C52/GKasso
INITIALS/SIG GKaser
DATE 10/8/09
ROUTING SYMBOL AJV-C5/GNielsen
INITIALS/SIG [illegible]
DATE [illegible]
ROUTING SYMBOL AJV-C/AKim
INITIALS/SIG AKim
DATE 10/8/09
ROUTING SYMBOL AJV-C/KNezer
INITIALS/SIG Lee
DATE 10/9/09
ROUTING SYMBOL ASW-2
INITIALS/SIG mer
DATE 10/11/09
ROUTING SYMBOL ASW-1
INITIALS/SIG
DATE
ROUTING SYMBOL
INITIALS/SIG
DATE