ASDI Full Audit Guideline
Federal Aviation Administration
Traffic Flow Management Program Office
Version 1.2 March 17, 2008

Purpose of this Document

This document is intended to provide guidance on the contents of the Aircraft Situation Display to Industry (ASDI) full audit procedure. An ASDI full audit is required when a subscriber distributes Class One undelayed data or receives the data directly from the FAA. The three levels of audit and the situations they apply to are described in "Overview of the ASDI Audit Process" (See reference 2). This document is not intended as an audit procedure. The specific IT security technologies deployed by the Class One data subscriber or employed to conduct the audit are also beyond the scope of the audit guidelines.

Responsibilities of Class One Subscribers Regarding ASDI Audits and any Data Distribution Chain

ASDI Class One data subscribers have the following responsibilities related to the audit, as well as the responsibilities delineated in the MOA.

- Maintain an active MOA with the FAA (direct subscribers). In the case of indirect subscribers, an agreement will be maintained with their direct subscriber.
- Keep their audit status current and implement audit recommendations in a timely fashion as specified by the FAA in response to the audit report.
- As described in the MOA, Section 7.2.8, they must maintain a current and historical list of all their data subscribers and the type of data they receive, if any exist. The list must be forwarded to the FAA ASDI/NASSI POC by March 1 each year.
- If they exist, verify that all of their Class One data recipients have a current audit status.
- If they exist, verify that all of their Class One data recipients have a current MOA agreement with the direct subscriber
- Maintain appropriate IT security to prevent unauthorized access of Class One data and maintain appropriate IT security between audits.

These responsibilities still apply when a Class One data subscriber obtains the data from another data subscriber instead of directly from the FAA.

Scope of Audit

The FAA's goal is to protect ASDI Class One data from source to end-user and ensure that it is only received by ASDI participants who have been authorized by the FAA to receive Class One data. The purpose of the audit is to verify that sufficient IT security exists to protect the FAA's data from unauthorized access.

The audit should cover all systems on the Class One data path. The audit should determine whether unauthorized access of Class One data is possible. The audit should also determine whether an attacker could gain control of one or more of the Class One data subscriber's systems and use it to gain unauthorized access of Class One data.

The audit should consist of a security policy review, a physical security review, a configuration review, vulnerability scans, a penetration test, and a review and verification of any Class One data recipients.

The critical characteristic of Class One data is that it is undelayed data; therefore protection of the data for longer periods of time than the delay is outside the scope of the audit. Currently the delay is 5 minutes. Long-term data storage, media transportation, and media sanitation are beyond the scope of the audit. Backup and recovery capabilities are beyond the scope of the audit.

Overall IT security of Class One data subscribers, for example how well they are protected from denial of service attacks, or the existence of a business continuity plan, is beyond the scope of the audit. The Class One data subscriber has the option of going beyond the FAA audit requirements. For example, the FAA does not require any evaluation of vulnerability to denial of service attacks, however a Class One data subscriber may have sound business reasons to have this included in their audit.

Eligibility Review

The auditor should determine whether subscriber is eligible to receive the level of data they are being given. The auditor should be given access to documentation proving the subscriber qualifies for Class One data as defined in the MOA, Section 5.2. Additionally, if the subscriber receives London data, documentation should be provided proving the eligibility for London data as detailed in the MOA, Section 10.

Security Policy Review

The auditor should determine whether a security policy exists and is appropriate. The auditor should obtain and evaluate copies of written security policies. Security policies should reflect industry standards. Employees should be aware of the policies and how they relate to their behavior. Actual practices should not diverge from the security policy. Security responsibilities should be formally assigned and security policies should include protecting Class One data from unauthorized access.

Physical Security Review

The auditor should determine whether physical access to equipment is restricted appropriately. Physical access to equipment that would allow access of Class One data should be restricted to authorized people.

Configuration Review

The auditor should conduct a network topology analysis. The auditor will need to work with the subscriber to gain a thorough understanding of the network topology. This should include understanding the Class One data path. The information should be obtained from interviews and existing documentation, but may be supplemented by network scanning. External network connections should be determined, including phone access to devices on the network and wireless network connections. Devices on the Class One data path, for example routers,

firewalls, and servers should be determined, so that their software versions and configurations can be analyzed.

The auditor should conduct a vulnerability scan. Vulnerability scanning tools should be used to scan from the external network. Vulnerability scanning tools should be used to scan internal systems. Sampling may be used to scan a subset of internal systems on the Class One data path when multiple systems perform identical functions. Manual commands may be used to complement automated tools and to eliminate false positives from the results.

The auditor should do a software analysis of systems on the Class One data path and protecting Class One data. Software versions and patch levels should be determined and evaluated. This should include installed applications, including web servers, as well as operating systems. Results of vulnerability scans should be used in the evaluation of software versions. Where appropriate virus and malware protection tools should be in use. Vulnerabilities that would not lead to unauthorized access of Class One data, such as DOS vulnerabilities, are not of concern. The systems should be evaluated for software vulnerabilities that would allow unauthorized use or control of the systems. A software update procedure should be in place to make sure that security updates are deployed promptly. Where appropriate automatic updates are configured. Where automatic updates are inappropriate, for example testing is required before applying patches; security updates are still applied promptly. Unnecessary applications should be removed.

The audit should conduct a security configuration analysis. Configuration of devices that could allow access to Class One data, such as routers, firewalls, and servers should be examined and evaluated. Unnecessary services should be disabled. Operating system security configurations should confirm to industry standards.

The auditor should verify that an appropriate password policy exists and is followed. Accounts without passwords and accounts with default passwords should not exist. Only strong passwords should be used. Passwords should be changed regularly.

The auditor should verify that appropriate audit trails exist. Components of the audit trail may include firewall logs, operating system logs, intrusion detection system logs, web server logs, database logs, or other logs as appropriate.

The auditor should analyze firewall policies and, if applicable, router access control policy and verify that they are based on deny-all with exceptions rather than allow-all with exceptions. Firewalls should use stateful inspection. Only required and documented traffic should be allowed in from the Internet. Internal addresses should not be allowed in from the Internet.

The auditor should verify that database server and web server configuration protects Class One data from unauthorized access.

Penetration Test

A penetration test is required. The penetration test should cover externally accessible IP addresses. The penetration test needs to test against external network attacks, but does not need to test against social engineering or physical break-ins, nor does the penetration testing need to be

covert. Where web servers are used to distribute Class One data the penetration test should attempt to take advantage of web server vulnerabilities.

Review and Verification of Class One Data Recipients

If the Class One data subscriber being audited redistributes Class One data, then the subscriber will supply the auditor with a listing and classification of any and all Class One data recipients. The auditor should both review the documentation and verify that only Class One data recipients actually receive Class One data.

The auditor should verify that data recipients receive the correct data type. For example, Class One display-only data recipients may not receive a digital feed of Class One data. For example, when a Class One data subscriber has both Class One and Class Two recipients the auditor should verify that Class Two data recipients cannot receive Class One data.

Report

The audit report delivered to the subscriber should include:

- Date(s) the audit was conducted
- Contact information of the auditee
- List of interviewees
- High-level description and/or diagram of the Class One data path including relevant network devices
- Evaluation of configuration review
- Evaluation of vulnerability scan results
- Results of penetration testing
- Results of Class One data recipient review
- Audit findings, significance, and recommendations

The audit report delivered to the FAA should include:

- Date(s) the audit was conducted
- Contact information of the auditee
- Audit findings, significance, and recommendations

References

1. "Memorandum of Agreement for Industry Access to the Aircraft Situation Display and National System Status Information Data," Federal Aviation Administration, June 1, 2006. This document, which must be signed by the ASDI direct subscriber, spells out the responsibilities of both the FAA and the direct subscriber. If the direct subscriber violates this MOA, then the direct subscriber is liable to lose access to the feed.

2. "Overview of the ASDI Audit Process," Version 1.2, March 13, 2007. This document includes a description of the three levels of ASDI audit, and how to determine the required level of audit.

For the latest versions of these and other ASDI documents, go to http://www.fly.faa.gov/ASDI/asdi.html

Contacts:
For more information about the ASDI Program, contact the ASDI Program Office at asdi-program-office@faa.gov.

ASDI Full Audit Checklist

The ASDI Full Audit Checklist is intended to be a high level list of areas that should be addressed by the audit. It is not intended to be a procedure. It is included to provide the Class One data subscriber and auditor with a checklist and quick reference on areas the audit should cover.

Item	Requirement	Comments	Comply Y/N
1.	The Class One data subscriber is eligible to receive the authorized Class One data.		
2.	Appropriate security policies exist and reflect industry standards.		
3.	Employees are aware of security policies and employee practices are consistent with security policies.		
4.	Security policies include protecting Class One data from unauthorized access.		
5.	Security authority and responsibilities are formally assigned.		
6.	Access to Class One data is limited to those authorized to access it.		
7.	Physical access to equipment that would allow access to Class One data is restricted to authorized personnel.		
8.	Class One data is only sent to ASDI participants authorized by the FAA to receive Class One data.		
9.	The network topology and the Class One data path are capable of protecting Class One data from unauthorized access. In most cases a network diagram will be required. Internet access points are firewalled. DMZ's are used and firewalled as appropriate to protect Class One data from unauthorized access.		
10.	Vulnerability scanning from the external network shows no vulnerabilities that would allow unauthorized access of Class One data.		

11.	Vulnerability scanning on internal systems on the Class One data path shows no vulnerabilities that would allow unauthorized access of Class One data.		
12.	Software versions and patch levels on systems on the Class One data path, including routers, firewalls, and systems, are adequate to protect Class One data from unauthorized access.		
13.	Application software versions and patch levels on systems on the Class One data path are adequate to protect Class One data from unauthorized access.		
14.	Appropriate software update procedures exist and are followed.		
15.	Outside sources are used to monitor the status of new security vulnerabilities applicable to protecting Class One data.		
16.	Software updates required to protect Class One data from unauthorized access are applied promptly. Automatic updates are used where appropriate.		
17.	Where appropriate virus and malware protection tools are used and kept up to date on systems on the Class One data path.		
18.	Unnecessary applications are not installed on systems on the Class One data path.		
19.	The security configuration of devices and systems on the Class One data path, for example routers, firewalls, systems, is hardened and adequate to protect Class One data from unauthorized access.		
20.	Unnecessary services are disabled on devices and systems on the Class One data path, for example on routers, firewalls, and systems.		
21.	Firewall and router security policies and rule sets are documented, restrictive, and based on least access, deny-all rules. Required services and ports are documented.		
22.	Firewalls use stateful inspection.		
23.	Only required and documented traffic is allowed in from the Internet.		
24.	Internal addresses are not allowed in from the Internet.		
25.	Modem and wireless polices and practices follow industry standards.		

26.	Account management policies and standards follow industry standards.		
27.	A strong password policy is used.		
28.	Passwords and security related pass phrases and identifiers are changed from the defaults.		
29.	Passwords are changed regularly.		
30.	Passwords conform to the strong password policy and are difficult to crack.		
31.	Audit trails exist, which may include firewall logs, operating system logs, intrusion detection system logs, web server logs, database server logs.		
32.	Database and web server application configurations protect Class One data from unauthorized access.		
33.	The Class One data subscriber is familiar with and follows the ASDI MOA.		
34.	Penetration testing against externally addressable IP addresses demonstrates that Class One data is adequately protected from unauthorized access.		
35.	Penetration testing against web servers that distribute Class One data demonstrates that Class One data is adequately protected from unauthorized access.		
36.	If the Class One data subscriber redistributes Class One data, all Class One data recipients are documented.		
37.	If the Class One data subscriber redistributes Class One data, only authorized Class One data recipient receive Class One data.		
38.	If the Class One data subscriber redistributes both Class One data and Class Two data, Class Two data recipients do not receive Class One data.		
39.	If the Class One data subscriber distributes Class One display-only Class One data, display-only data recipients do not receive the Class One digital data feed.		