DIA Information Security Management
Performance Audit

November 2010

Office of the Auditor
Audit Services Division
City and County of Denver

Dennis J. Gallagher
Auditor
The **Auditor** of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver’s government. He also chairs the City’s Audit Committee and oversees the City’s Comprehensive Annual Financial Report (CAFR)

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

**Audit Committee**

Dennis Gallagher, Chair  
Maurice Goodgaine  
Jeffrey Hart  
Timothy O’Brien

Robert Bishop  
Robert Haddock  
Bonney Lopez

**Audit Staff**

Audrey Donovan, Deputy Director, CIA  
Stephen E. Coury, IT Audit Supervisor, CISA  
Robert Pierce, Lead IT Auditor, CISA  
Aaron Pratt, Senior IT Auditor, CISA

You can obtain free copies of this report by contacting us at:

**Office of the Auditor**

201 West Colfax Avenue, Department 705  •  Denver CO, 80202  
(720) 913-5000  •  Fax (720) 913-5026

Or download and view an electronic copy by visiting our website at:

[www.denvergov.org/auditor](http://www.denvergov.org/auditor)
Ms. Kim Day, Manager  
Department of Aviation  
City and County of Denver

Dear Ms. Day:

Attached is the Auditor’s Office Audit Services Division’s report of their audit of Information Security Management at Denver International Airport for the period of January 1, 2009 through August 31, 2010. The purpose of the audit was to examine and assess the effectiveness and efficiency of controls related to information security management, information systems access management, and contingency planning.

Audit work revealed weaknesses with policies, standards, and procedures related to information security practices across some airport divisions resulting in several controls being ineffective or missing entirely. Clarifying who has authority for oversight and enforcement of airport-wide information security policies, standards, and procedures will promote wider acceptance of information technology governance risk management practices and improve the efficiency of developing stronger, more mature, and consistent process controls.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5029.

Sincerely,

Dennis J. Gallagher  
Auditor

cc: Honorable John Hickenlooper, Mayor  
Honorable Members of City Council  
Members of Audit Committee  
Ms. Roxane White, Chief of Staff  
Mr. Claude Pumilia, Chief Financial Officer  
Mr. David Fine, City Attorney  
Mr. L. Michael Henry, Staff Director, Board of Ethics  
Ms. Lauri Dannemiller, City Council Executive Staff Director

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people.

We will monitor and report on recommendations and progress towards their implementation.
To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people.

We will monitor and report on recommendations and progress towards their implementation.
AUDITOR’S REPORT

We have completed an audit of Information Security Management at Denver International Airport for the period January 1, 2009 through August 31, 2010. The purpose of the audit was to examine and assess the effectiveness and efficiency of controls related to information security management, information systems access management, and contingency planning.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit work revealed weaknesses with policies, standards, and procedures related to information security practices across some airport divisions resulting in several controls being ineffective or missing entirely. Clarifying who has authority for oversight and enforcement of airport-wide information security policies, standards, and procedures will promote wider acceptance of information technology governance risk management practices and improve the efficiency of developing stronger, more mature, and consistent process controls.

We extend our appreciation to the personnel who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CICA
Director of Audit Services
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY**  
Opportunities Exist to Enhance DIA Information Technology Governance and Process Maturity  

**INTRODUCTION & BACKGROUND**  
The Denver International Airport  
Critical Systems at DIA  
Distinguishing Between Criticality and Safety  
Systems Selected for Audit Testing  
What is Information Security Management?  
Information Security Management at DIA  
Information Technology Governance Maturity Model  
Information Systems Access Management at DIA  
Contingency Planning  
Contingency Planning at DIA  

**SCOPE**  

**OBJECTIVES**  

**METHODOLOGY**  

**FINDINGS**  
Opportunities Exist to Enhance DIA Information Technology Governance and Process Maturity  

**RECOMMENDATIONS**  

**AGENCY RESPONSE**
EXECUTIVE SUMMARY

Opportunities Exist to Enhance DIA Information Technology Governance and Process Maturity

Audit work revealed weaknesses with policies, standards, and procedures related to information security practices across some airport divisions resulting in several controls being ineffective or missing entirely.

We selected three systems from three separate divisions of the airport that have high availability requirements. We utilized the principles of defense in depth\(^1\) and evaluated process maturity in the areas of information security management, information systems access management, and contingency planning. Control deficiencies were noted within each area we reviewed.

On the other hand, our testing to ensure that employee badges and system access are disabled when personnel terminate employment found no exceptions for badges and only one exception for system access, demonstrating that strong controls exist for removing physical access and system access when personnel terminate their employment.

The audit discovered control weaknesses in the following areas:

- **Server and workstation patching and antivirus protection** – Workstations that are not patched against known system vulnerabilities or do not have their antivirus software up to date could be susceptible to malicious computer software that may facilitate unauthorized access and the subsequent disclosure, misuse or destruction of sensitive City information.

- **System backups** – Without offsite backups, it may not be possible to recover critical systems.

- **User IDs and password strength** – The use of generic user IDs or weak passwords may lead to unauthorized access and do not support individual accountability for system access.

- **Physical security, hardware maintenance, and environmental controls** – Weak controls in these areas do not provide accountability for access to a data center, support timely repair of computer hardware, or ensure a proper operating temperature for continued operation of computer equipment.

- **Formal contingency plans** – Formally documented and tested contingency plans can improve the likelihood that critical airport systems can be recovered in the event of a significant system failure or disaster. If a critical system is not recovered in a reasonable amount of time, there could be an adverse impact on flight operations, financial accounting, passenger experience, and airport reputation.

\(^1\) Defense in depth is the use of multiple layers of physical, policy, and technical controls to mitigate information security risk.
Clarifying who has authority for oversight and enforcement of airport-wide information security policies, standards, and procedures will promote wider acceptance of information technology governance risk management practices and improve the efficiency of developing stronger, more mature, and consistent process controls.
INTRODUCTION & BACKGROUND

The Denver International Airport

The City and County of Denver owns and operates the Denver International Airport (DIA). The facility opened on February 28, 1995 and is now the nation’s fifth busiest airport.2 DIA’s construction utilized novel building materials such as Teflon-coated fiberglass to create its distinctive appearance resembling snow covered mountain peaks.

The airport was also built during a time when security measures for aviation were under close scrutiny. This allowed the designers of the airport to plan for the integration of passenger and baggage screening in a way supporting efficient passenger movement and the placement of checked baggage handling away from traveler areas.

All operations of the airport are within the City’s Department of Aviation which is led by the Manager of Aviation, who is appointed by and reports to the Mayor of Denver.

Critical Systems at DIA

The airport is comprised of many information and process control systems, of which some are interdependent upon one another. Examples of a few systems that are involved in the business of running the airport include:

- Parking fees
- Financial accounting
- Checked baggage handling
- Network and communications
- Access control and alarm monitoring
- Automated concourse passenger train
- Departure and arrival information displays
- Emergency response (police, fire, ambulance)

---

2 Based on CY 2009 FAA passenger boarding (enplanement) statistics
http://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/
These airport systems all contribute to maintaining efficient and smooth operations. As such, the unavailability or failure of certain systems, be it temporary or long-term, would cause significant traveler inconvenience, financial impact to the airport and airlines, reputational damage, or air traffic interruption.

Distinguishing Between Criticality and Safety

Critical systems referred to in this audit pertain to those that must remain available (up and running) to maintain smooth and efficient airport operations. Air space safety on the other hand, although a key mission of the airport, is primarily the responsibility of the Transportation Security Administration (TSA). In addition, the control of aircraft landings and take-offs are the responsibility of the Federal Aviation Administration (FAA).

The airport is required to meet both TSA & FAA regulatory requirements, and provides infrastructure and information and process control systems that allow TSA to accomplish its air space safety objectives and the FAA to meet its flight control objectives. If any supporting airport system fails to meet TSA & FAA requirements, both TSA and FAA have the authority to cease flight operations. Although there is a clear separation of responsibilities, there is a critical interdependence of infrastructure, communications, information, and process control systems for the airport to remain operational.

Systems Selected for Audit Testing

The management and operation of the airport’s diverse systems falls into the various functional divisions of the airport. For audit testing, we selected from three separate divisions, the following distinctly different information and process control systems:

- Access Control and Alarm Monitoring System (ACAMS)
- AMS Financial System (AMS)
- Baggage Handling System (BHS)

Following is a high level overview of what each system accomplishes for the airport.

Access Control and Alarm Monitoring System (ACAMS)

DIA operates an access control and alarm monitoring system which is used to control the passage of personnel (not passengers) into secure and sterile airport areas in line with TSA regulatory requirements and DIA’s specific Airport Security Program. The system includes door badge readers, biometric sensors, road access gates, and visual identification badges. The system is also supplemented by security guards, as well as, audio and video monitoring.

DIA is obligated to inform TSA and FAA of any significant outages in ACAMS. Those agencies then determine whether flight operations can continue. In the worst case
scenario, the airport could be shut down if this system does not meet operational requirements.

**AMS Financial System (AMS)**

The American Management System (AMS) serves as DIA’s financial system of record for general ledger, accounts receivable, accounts payable, fixed assets, and projects.

In 2009, there were over $564 million in revenues\(^3\) processed through AMS. Although there are daily summary transactions transmitted to PeopleSoft, the City and County of Denver’s financial system of record, PeopleSoft serves only as a historical record and cannot be used to process transactions.

In the event a disaster prevented the timely recovery of AMS, the airport would be significantly hindered in meeting its financial and reporting requirements.

**Baggage Handling System (BHS)**

The Baggage Handling System (BHS) is used to control the vast and complex arrays of conveyor belts that move passenger-checked bags through the automated Explosives Detection System (EDS) operated by the TSA. The system itself does not control the screening of baggage but rather supports the directives given by TSA to route bags for loading onto aircraft, holding bags for further TSA analysis, and delivering bags to TSA personnel for manual inspection. Should the BHS fail for an extended period of time, passengers would be inconvenienced as their checked bags may not be on their flight.

---

\(^3\) City and County of Denver Municipal Airport System Annual Financial Report, December 31, 2009 and 2008
What is Information Security Management?

A widely adopted model of information security is based on the three concepts of confidentiality, integrity, and availability (or CIA).

**Confidentiality** relates to restricting access to those persons authorized in order to protect privacy. Common techniques to control access are through the use of user IDs and passwords.

**Integrity** controls prevent the improper modification or destruction of information. Access privileges or permissions are a common way of controlling who can read or update data.

**Availability** ensures timely and reliable access to and use of information. Contingency plans provide ways that data can be restored in the event that a catastrophic event inhibits access to systems.

Information security management includes a myriad of activities that help accomplish the above CIA objectives, such as, defining policies, standards, and procedures, conducting security threat assessments, monitoring system access, establishing user IDs, changing passwords, and planning for contingencies.

Best practices promote the concept of “defense in depth” or “security in layers.” Security programs should protect information through the use of physical, policy, and technical controls. The security program should also ensure that technical controls are not too narrowly focused or overly rely on limited defenses, such as firewalls or workstation software patching. The security program needs to include all aspects of security such as video monitoring, reviews of logs, and employee security awareness training. Information risk management also requires a vigilant ongoing program to constantly assess emerging and persistent risks in light of an ever changing threat horizon.

**Information Security Management at DIA**

The Information Technologies Division is headed by the Chief Information Officer (CIO), who is a deputy manager and reports to the airport’s Manager of Aviation. The Information Technologies Division provides technical and operational support for many of the business systems running at the airport. They also lend technical support staff to other divisions. However, some divisions, at least partially, support their own technology needs. Of the systems we selected for audit, the Information Technologies Division partially supports the ACAMS system, entirely supports the AMS system, and supports only network access for the Baggage Handling System.
DIA’s Information Technologies Division has developed some formally documented information security standards. These standards are based largely on guidance available from the National Institute of Standards and Technology (NIST) Computer Security Resource Center. NIST offers a series of “special publications” (800 Series) that represent best practices resulting from collaboration of industry, government, and academic organizations.4

Established within the Information Technologies Division is the role of the Chief Information Security Officer (CISO) who is responsible for overseeing the DIA Information Security Program with the objective of preserving the confidentiality, integrity and availability of all data being stored or processed on the DIA networks.

**Information Technology Governance Maturity Model**

Information Technology (IT) Governance consists of the five major domains of strategic alignment, value delivery, risk management, resource management, and performance measurement. The main focus of this audit was risk management, which addresses the safeguarding of IT assets, disaster recovery and continuity of operations.5

We evaluated key information security policies, standards, and procedures against an industry standard IT governance maturity model. As illustrated below, the model establishes a method to rank a process along a six point scale ranging from “0 – Nonexistent” to “5 – Optimized.”

---

5 Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, http://www.itgi.org
Information Systems Access Management at DIA

Employees are issued user IDs and passwords which grant them access rights to DIA's information systems. Access is disabled or removed when individuals terminate their employment. These controls are designed to ensure that only authorized individuals have access to DIA systems and data.

Contingency Planning

Guidance in the Contingency Planning Guide for Federal Information Systems (NIST SP800-34) states, “Effective contingency planning begins with the development of an organization contingency planning policy and subjection of each information system to a business impact analysis (BIA).” This process ensures that contingency plans are commensurate with the risk faced by the business. The BIA should address items like the age of computer equipment, dependency on key personnel, the likelihood of natural disasters, etc. The BIA for any given system should include the input from other divisions so that a balanced view of risk is obtained. For example, one division may rank the risk of its applications low, but these same system risks may have a higher impact outside of the division that would warrant the risks being rated higher from an organizational perspective.

The above diagram illustrates the seven step process for contingency planning, including testing the plan and keeping it current.

Contingency Planning at DIA

DIA is responsible for maintaining certain infrastructure that is necessary for the TSA to accomplish its airspace security objectives and for the FAA to manage flights. Should any of those systems fail, DIA must promptly notify the appropriate agencies of the extent of the failure. The agencies then assess the issue and determine whether the airport will be allowed to continue flight operations.

Although TSA requirements address airport contingency plans, they do not require formal contingency plans for specific application systems. However, documents published by the TSA provide guidance to airports to ensure systems are protected in order to avert disruption of operations and inconvenience to the public.

---

6 Contingency Planning Guide for Federal Information Systems, National Institute of Standards and Technology, Special Publication 800-34, (NIST SP800-34)
7 Code of Federal Regulations, Title 49 Transportation, Part 1542 Airport Security
8 Transportation Security Administration, Recommended Security Guidelines for Airport Planning, Design and Construction, Revised June 15, 2006
SCOPE

The audit examined and assessed the effectiveness and efficiency of controls at Denver International Airport related to information security management, information systems access management, and contingency planning. Systems deemed in scope included; the Access Control and Alarm Monitoring System (ACAMS), American Management System (AMS), and the Baggage Handling System (BHS). The audit period extended from January 1, 2009 through August 31, 2010.

In accordance with Generally Accepted Government Auditing Standards (GAGAS) the reader should be aware that some details about information security weaknesses are considered sensitive security information and are not disclosed within this report. TSA regulation (CFR 49, section 1520.5) also restricts the discussion of sensitive security information.9

The details of all findings, however, have been discussed with DIA senior staff and management. As part of our regular follow-up for audit issues, we will return at a future date to ensure all findings have been addressed.

OBJECTIVES

The audit objectives were to ensure the following:

- Physical and logical access to critical system infrastructure is restricted to authorized personnel.
- Contingency plans and processes are in place for critical DIA systems.
- Security patch levels and antivirus definitions are up to date.
- Backups are created and stored off-site for critical systems.
- Data centers and hardware associated with critical DIA applications are managed at a level commensurate with the availability requirements of the respective systems.
- Terminated employees have their access removed or disabled upon termination.
- Policies, standards, and procedures define responsibilities for information security management.

9 Code of Federal Regulations, Title 49 Transportation, Part 1520 Protection of Sensitive Security Information
METHODOLOGY

We utilized the principles of defense in depth and evaluated process maturity in the areas of information security management, information systems access management, and contingency planning.

We utilized four main audit and control frameworks and guidelines including:

- Federal Information Security Controls Audit Manual (FISCAM) issued by the Government Accountability Office\(^\text{10}\)
- National Institute of Standards & Technology (NIST) – Computer Security Resource Center. NIST “special publications” SP 800 series\(^\text{11}\)
- Transportation Security Administration (TSA) – Recommended Security Guidelines for Airport Planning, Design and Construction\(^\text{12}\), and related TSA Regulations\(^\text{13}\)
- Information Technology Governance Institute (ITGI) — IT Governance Maturity Model\(^\text{14}\)

The evidence gathering and analysis techniques used to meet our audit objectives included, but were not limited to:

- Interviewing personnel in Information Technologies, Finance, Airport Legal Services, Operations, Physical Security, and vendors associated with critical airport systems;
- Reviewing organizational charts and system inventories;
- Identifying critical applications in use at DIA;
- Examining policies, standards, and procedures for physical and logical access;
- Utilizing Computer Assisted Auditing Techniques (CAATs), including ACL (a data analytics software package) to compare 1,248 employee terminations from PeopleSoft Human Resources (HR) to the physical access badges issued in ACAMS and user ID access lists, such as, Active Directory;
- Reviewing antivirus definitions and security patch levels;
- Observing environmental controls for critical information and process control systems;
- Reviewing the adequacy of hardware maintenance arrangements;
- Reviewing backup processes;
- Reviewing for contingency plans and business impact analyses; and
- Reviewing external auditor reports.

---


\(^{11}\) National Institute of Standards and Technology, Computer Security Resource Center, Special Publications (800 Series)

\(^{12}\) Transportation Security Administration, Recommended Security Guidelines for Airport Planning, Design and Construction, Revised June 15, 2006

\(^{13}\) Code of Federal Regulations, Title 49 Transportation, Part 1542 Airport Security

\(^{14}\) Board Briefing on IT Governance, 2nd Edition, IT Governance Institute
FINDINGS

Opportunities Exist to Enhance DIA Information Technology Governance and Process Maturity

Audit work revealed weaknesses with policies, standards, and procedures related to information security practices across some airport divisions resulting in some controls being ineffective or missing entirely.

We selected three systems with high availability requirements from three separate divisions of the airport. We utilized the principles of defense in depth and evaluated process maturity in the areas of information security management, information systems access management, and contingency planning.

We observed that while some divisions had standards for information security management, they were not disseminated to the other divisions; as a result, they were not uniformly adopted or followed. This situation resulted in control gaps and disparities in the relative maturity of process controls, which were not commensurate with system criticality or availability requirements. Following is a summary of identified control deficiencies.

- **Server and workstation patching and antivirus protection** – Some servers and workstations were not being patched or protected against computer viruses. Some of these machines were located on isolated networks without Internet or e-mail access which helped to mitigate some risk. However, workstations that are not patched against known system vulnerabilities or do not have their antivirus software up to date could be susceptible to malicious computer software that may facilitate unauthorized access and the subsequent disclosure, misuse or destruction of sensitive City information.

- **System backups** – Some systems did not have backups stored offsite. In the event of a data center fire, flood, or disaster, there is a risk that the backup media could be destroyed along with the hardware. Without offsite backups, it may not be possible to recover critical systems.

- **User IDs and password strength** – Some systems did not have adequate user ID and password strength or complexity requirements. The use of generic user IDs or weak passwords may lead to unauthorized access and do not support individual accountability for system access.

- **Physical security, hardware maintenance, and environmental controls** – A data center did not have physical access controls to support individual accountability for room access, sufficient hardware maintenance arrangements to ensure timely repair in the event of hardware malfunctions, or adequate cooling for computer equipment to ensure machines do not overheat and shut down.

- **Formal contingency plans** – Some systems did not have formal and tested contingency plans in place. There is no single person or department with primary
responsibility for developing Continuity of Operations (COOP) plans for the entire airport. Formally documented and tested contingency plans can improve the likelihood that critical airport systems can be recovered in the event of a significant system failure or disaster. Contingency planning needs to be an ongoing activity or a recurring project to ensure that plans stay current as processes and systems evolve. If a critical system is not recovered in a reasonable amount of time, there could be an adverse impact on flight operations, financial accounting, passenger experience, and airport reputation.

RECOMMENDATIONS

1. IT Governance and Process Maturity

Senior staff, such as the CIO, CISO, CTO, CFO and division managers, reporting to the Manager of Aviation should clarify who has authority for oversight and enforcement of airport-wide information security policies, standards, and procedures. This action will promote wider acceptance of IT governance risk management practices and improve the efficiency of developing stronger, more mature, and consistent process controls.

2. Server and workstation patching and antivirus protection

Senior staff should adopt policies, standards, and procedures to ensure the successful application of security patches and antivirus updates.

3. System backups

Senior staff should ensure policies, standards, and procedures support offsite storage of critical system backups.

4. User IDs and password strength

Senior staff should ensure policies, standards, and procedures adequately support individual user accountability including the use of strong passwords.

5. Physical security, hardware maintenance, and environmental controls

System owners should provide accountability for physical access to the data center room, ensure hardware is under adequate maintenance agreements, and improve the data center environmental controls.

6. Formal contingency plans

Senior staff should issue a policy requiring that all airport systems have contingency plans in accordance with overall risk as determined through a business impact analysis.
AGENCY RESPONSE

Audit Response Letter

November 1, 2010

Mr. Kip R. Memmott, MA, CGAP, CICA
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of DIA Information Security Management for the audit period beginning January 1, 2009 through August 31, 2010.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on October 11, 2010. This response complies with Section 20-276 (b) of the Denver Revised Municipal Code (DRMC).

AUDIT FINDING: Opportunities Exist to Enhance DIA Information Technology Governance and Process Maturity
RECOMMENDATION 1: IT Governance and Process Maturity

Senior staff, such as the CIO, CISO, CTO, CFO and division managers, reporting to the Manager of Aviation should clarify who has authority for oversight and enforcement of airport-wide information security policies, standards, and procedures. This action will promote wider acceptance of IT governance risk management practices and improve the efficiency of developing stronger, more mature, and consistent process controls.

 RESPONSE/ACTION PLAN:

- The Technologies Division shall draft DIA 8001 – Information Security Program Grant of Authority, which identifies roles and responsibilities throughout DIA with regard to the governance of an airport-wide Information Security Program (ISP), including the creation, oversight and enforcement of airport-wide Information Security policies, standards and procedures. (Complete)

- Senior Staff shall review, provide input, and approve DIA 8001 – Information Security Program Grant of Authority.

- The Information Security Program shall be socialized throughout DIA Divisions and shall be published internally and made available to all employees, contractors and vendors with Intranet access.

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>DIA 8001 Approval December 31, 2010</td>
<td>Robert Kastelitz 303.342.2020</td>
</tr>
<tr>
<td></td>
<td>DIA 8001 Publication and Socialization March 31, 2011</td>
<td>Brian Monroe 303.342.2065</td>
</tr>
</tbody>
</table>
RECOMMENDATION 2: Server and workstation patching and antivirus protection

Senior staff should adopt policies, standards, and procedures to ensure the successful application of security patches and antivirus updates.

➢ RESPONSE/ACTION PLAN:

  o Patching and antivirus protection are part of the proposed ISP (see recommendation above).

  o DIA will socialize the ISP to all users and agencies who connect systems to DIA’s network computing infrastructure which are subject to DIA Technologies governance (see recommendation 1 above).

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Patching standard and processes in place - March 31, 2011</td>
<td>Brian Monroe 303.342.2065</td>
</tr>
<tr>
<td></td>
<td>Socialization and publication – March 31, 2011</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brian Monroe</td>
</tr>
</tbody>
</table>
RECOMMENDATION 3: System backups

Senior staff should ensure policies, standards, and procedures support offsite storage of critical system backups.

➢ RESPONSE/ACTION PLAN:

- DIA Technologies shall create policies, standards and procedures to support offsite storage of critical system backups, or for acceptable alternatives based on business requirements.

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Procedures in place – June 30, 2011</td>
<td>Mike Wright 303.342.2002</td>
</tr>
</tbody>
</table>
RECOMMENDATION 4: User IDs and password strength

Senior staff should ensure policies, standards, and procedures adequately support individual user accountability including the use of strong passwords.

➢ RESPONSE/ACTION PLAN:

   o Unique User ID use and password strength standards and enforcement are part of the proposed ISP (See recommendation 1 above).

   o DIA will socialize the ISP to all users and agencies who connect systems to DIA’s network computing infrastructure which are subject to DIA governance.

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>ISP in place March 31, 2011</td>
<td>Brian Monroe 303.342.2065</td>
</tr>
<tr>
<td></td>
<td>ISP published and socialized March 31, 2011</td>
<td>Brian Monroe</td>
</tr>
</tbody>
</table>
RECOMMENDATION 5: Physical security, hardware maintenance, and environmental controls

System owners should provide accountability for physical access to the data center room, ensure hardware is under adequate maintenance agreements, and improve the data center environmental controls.

➢ RESPONSE/ACTION PLAN:

- All access doors to data center rooms shall have badge readers installed. Doors directly from the data center to publicly accessible areas shall be disabled, buffered or configured for emergency access only.

- Agreements shall be put in place or hardware shall be upgraded to ensure all critical systems are under hardware maintenance support agreements.

- Data center environmental controls shall be reviewed and upgraded as necessary to minimize risk to critical systems due to environmental factors.

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware for all critical systems reviewed for maintenance – March 31, 2011</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data center environmental controls June 30, 2011</td>
<td>Mike Wright (and Richard Kelly)</td>
</tr>
</tbody>
</table>
RECOMMENDATION 6: Formal contingency plans

Senior staff should issue a policy requiring that all airport systems have contingency plans in accordance with overall risk as determined through a business impact analysis.

➢ RESPONSE/ACTION PLAN:

  o Technologies shall draft a policy to this effect.

  o The policy shall be reviewed and approved by Senior Staff.

  o The contingency program shall be governed by Technologies' Office of the CIO and implemented by Technologies staff, or other technology staff as needed.

  o The Information Assurance Team shall monitor systems for compliance commensurate with their criticality.

<table>
<thead>
<tr>
<th>State your agreement or reason for disagreement with Recommendation</th>
<th>Target date to complete implementation activities (Generally Expected within 60 to 90 days)</th>
<th>Name and phone number of primary individual responsible for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------</td>
<td>-----------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>Contingency plan development for critical systems – June 31, 2011</td>
<td>Brian Monroe 303.342.2065</td>
</tr>
<tr>
<td></td>
<td>Contingency plan implementation for critical systems December 30, 2011</td>
<td>Mike Wright</td>
</tr>
</tbody>
</table>

Please contact Robert Kastelitz at 303.342.2020 with any questions.

Sincerely,

Robert W. Kastelitz
City and County of Denver
Department of Aviation
Deputy Manager of Technologies

cc: Kim Day
Xavier DuRán
Dave Rhodes
Patrick Heck
Mark Nagel
Brian Monroe
Mike Wright
Les Berry
Brian Elms
Rick Kelly