OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 20, 2014

MEMORANDUM FOR: CHARLES L. MCGANN, JR.
MANAGER, CORPORATE INFORMATION SECURITY

Kevin H Ellenberger

for

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Information Technology and Data Analysis

SUBJECT: Management Alert – Backup and Recovery of Essential Data
(Report Number IT-MA-14-001)

This management alert presents our review of backup and recovery procedures for essential databases due to a recent hardware failure that resulted in a loss of Computer Incident Response Team (CIRT) data (Project Number 14BM003IT001). This issue came to our attention during our Fiscal Year 2014 Information Technology Internal Controls audit (Project Number 14BM003IT000).

We appreciate the cooperation and courtesies provided by your staff and commend the immediate action taken by your office to ensure that CIRT data is maintained going forward. If you have any questions or need additional information, please contact Aron Alexander, director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Introduction

During the Fiscal Year (FY) 2014 Information Technology Internal Controls audit (Project Number 14BM003IT000), the U.S. Postal Service Office of Inspector General (OIG) became aware of a hardware failure that resulted in the loss of the Computer Incident Response Team (CIRT) database used to record and monitor computer incidents (Project Number 14BM003IT001).[1]

The U.S. Postal Service's Data Management Services group periodically performs off-site backups for hundreds of critical databases. However, there are other essential databases that are not classified as critical[2] that are used for daily functions. These functions include analysis of historical data and maintaining records for compliance with existing security policy.[3] We are issuing this alert to make the Postal Service aware of the need to modify its current backup and storage requirements to ensure that essential, but not critical, data is available.

Conclusion

The Postal Service did not ensure all database backups were being stored on separate hardware. Specifically, the CIRT database was lost due to a hardware failure and the data was not recovered due to the absence of a backup on a separate piece of hardware. As a result, this database was not available to perform historical analyses and the Postal Service could not comply with security policy. Although the Postal Service took immediate corrective action for this database by implementing backup procedures on separate hardware, there may be other unidentified databases that are not backed up on separate hardware that could result in a loss of data and the inability to comply with record maintenance requirements.

Backup and Recovery

The Postal Service maintained an essential CIRT database and backed up a copy of the database on the same hardware. On April 4, 2014, a hardware failure occurred that made the original database and the backup of the database inaccessible. [4] As a result, the database was not available to perform analyses of computer incidents that would enable management to more effectively monitor and resolve new incidents in a timely manner. In addition, the Postal Service could not maintain an electronic incident repository.

[1] Security incidents are events that threaten the integrity, availability, or confidentiality of information resources, such as suspicion or occurrence of any fraudulent activity; unauthorized disclosure, modification, misuse, or inappropriate disposal of Postal Service information.

[2] Information is designated as critical information if its unavailability would have a serious adverse impact on communications. Essential databases are necessary for daily operations, but are not classified as critical.

[3] Handbook AS-805, *Information Security*, Section 13-4.2.2 Processing Incidents Reports.

[4] The Postal Service maintained paper copies of incident reports that contained portions of the data lost.

Although management responded swiftly and took corrective action by updating and implementing backup procedures for a new CIRT database using the [redacted][5] application, there may be other essential databases used by other groups that are not backed up on separate hardware. The practice of backing up data on the same hardware could result in the loss of essential data, increased workhours to recreate the databases, and an inability to perform analyses in the event of hardware failure.

Currently, the Postal Service's security standards[6] state critical information resources must be stored off-site at a location that is not subject to the same threats as the original media, but does not prohibit the practice of using the same hardware to maintain and back up noncritical information resources. If the standards were updated, database owners would need to review and possibly modify their backup procedures, thereby ensuring information resources can be restored in a timely manner in the event of a hardware failure.

Recommendations

We recommend the manager, Corporate Information Security:

1. Expand existing procedures in Handbook AS-805, *Information Security,* to prohibit the practice of using the same hardware to maintain and back up noncritical information resources.

2. Issue a reminder that data backups are to be maintained in an appropriate location to reduce potential loss, damage, or misuse of essential data.

Management's Comments

Management agreed with the findings (in subsequent communications) and the recommendations in the report. Regarding recommendation 1, management stated Corporate Information Security will update Handbook AS-805, for backup storage requirements. Specifically, the policy will require that backups must not be stored on the same hardware device as the original information. Additionally, management will update off-site backup storage requirements to state that noncritical information stored on mainframes, servers, workstations, and mobile devices should be backed up and stored off-site at a location that is not subject to the same threats as the original information. Management's target implementation date is April 2015.

Regarding recommendation 2, management stated after updating Handbook AS-805, they will publish an article to Postal Service staff reminding them that backup media containing sensitive and non-publicly available information must be labeled as "Restricted Information" and backups must not be stored on the same hardware device as the original information. Management's target implementation date is April 2015. See Appendix A for management's comments, in their entirety.

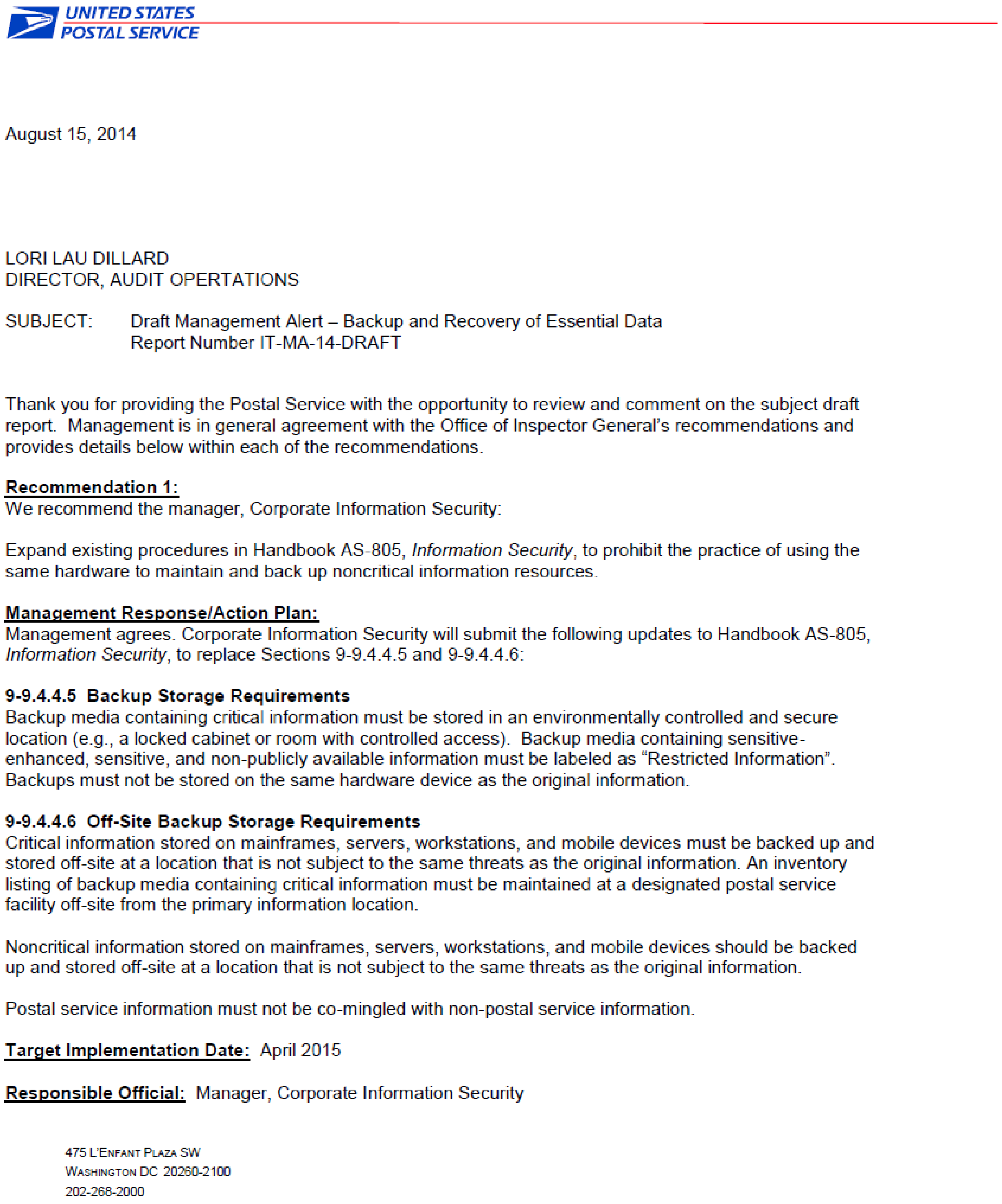
[5] [redacted] automates remote data backups.
[6] Handbook AS-805, *Information Security*, Section 9-9.4.4.6 Off-Site Backup Storage Requirements.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report.

The OIG considers all the recommendations significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendix A: Management's Comments



UNITED STATES
POSTAL SERVICE

August 15, 2014

LORI LAU DILLARD
DIRECTOR, AUDIT OPERTATIONS

SUBJECT: Draft Management Alert – Backup and Recovery of Essential Data
Report Number IT-MA-14-DRAFT

Thank you for providing the Postal Service with the opportunity to review and comment on the subject draft report. Management is in general agreement with the Office of Inspector General's recommendations and provides details below within each of the recommendations.

Recommendation 1:
We recommend the manager, Corporate Information Security:

Expand existing procedures in Handbook AS-805, *Information Security*, to prohibit the practice of using the same hardware to maintain and back up noncritical information resources.

Management Response/Action Plan:
Management agrees. Corporate Information Security will submit the following updates to Handbook AS-805, *Information Security*, to replace Sections 9-9.4.4.5 and 9-9.4.4.6:

9-9.4.4.5 Backup Storage Requirements
Backup media containing critical information must be stored in an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access). Backup media containing sensitive-enhanced, sensitive, and non-publicly available information must be labeled as "Restricted Information". Backups must not be stored on the same hardware device as the original information.

9-9.4.4.6 Off-Site Backup Storage Requirements
Critical information stored on mainframes, servers, workstations, and mobile devices must be backed up and stored off-site at a location that is not subject to the same threats as the original information. An inventory listing of backup media containing critical information must be maintained at a designated postal service facility off-site from the primary information location.

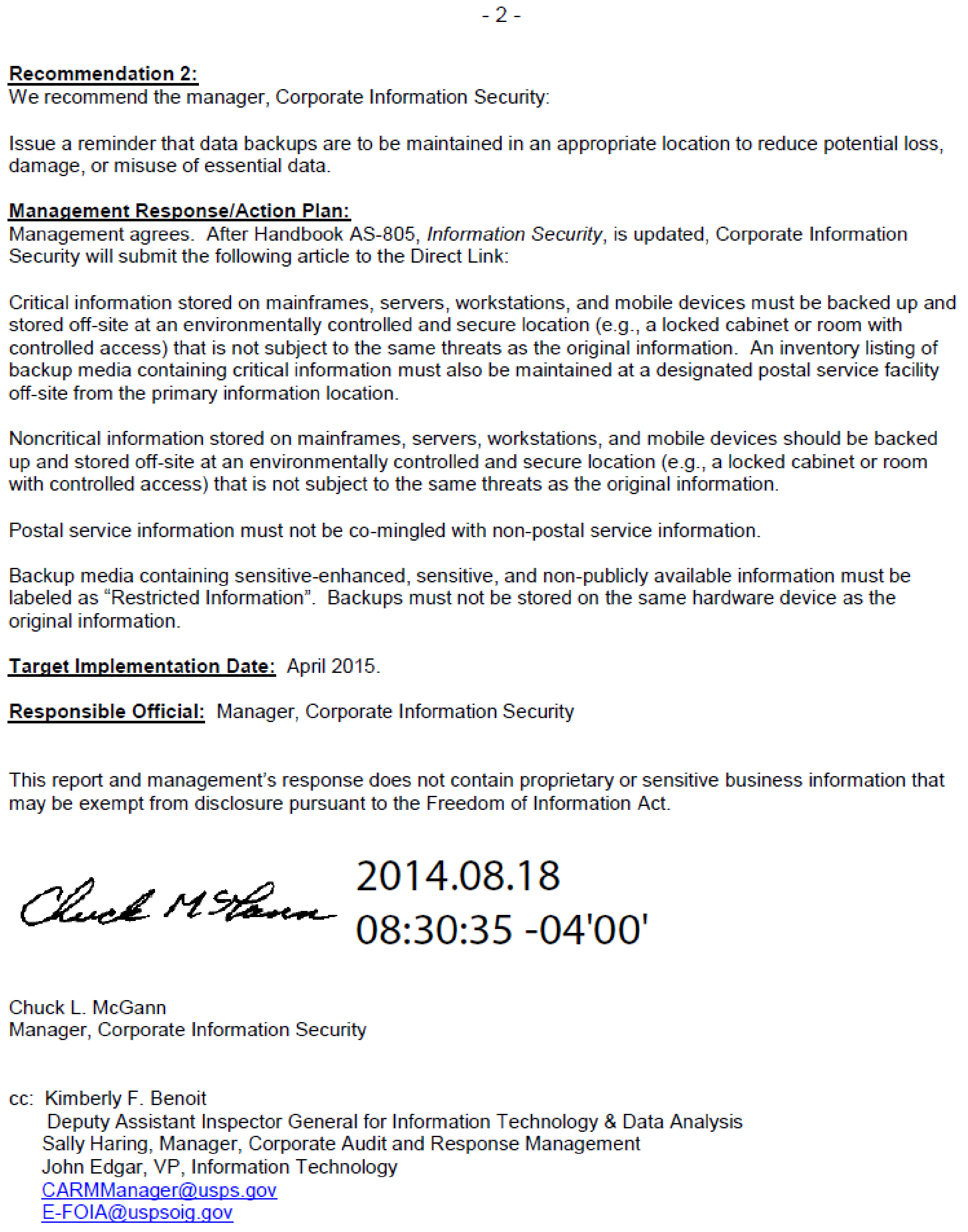
Noncritical information stored on mainframes, servers, workstations, and mobile devices should be backed up and stored off-site at a location that is not subject to the same threats as the original information.

Postal service information must not be co-mingled with non-postal service information.

Target Implementation Date: April 2015

Responsible Official: Manager, Corporate Information Security

475 L'Enfant Plaza SW
Washington DC 20260-2100
202-268-2000



- 2 -

Recommendation 2:
We recommend the manager, Corporate Information Security:

Issue a reminder that data backups are to be maintained in an appropriate location to reduce potential loss, damage, or misuse of essential data.

Management Response/Action Plan:
Management agrees. After Handbook AS-805, *Information Security*, is updated, Corporate Information Security will submit the following article to the Direct Link:

Critical information stored on mainframes, servers, workstations, and mobile devices must be backed up and stored off-site at an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access) that is not subject to the same threats as the original information. An inventory listing of backup media containing critical information must also be maintained at a designated postal service facility off-site from the primary information location.

Noncritical information stored on mainframes, servers, workstations, and mobile devices should be backed up and stored off-site at an environmentally controlled and secure location (e.g., a locked cabinet or room with controlled access) that is not subject to the same threats as the original information.

Postal service information must not be co-mingled with non-postal service information.

Backup media containing sensitive-enhanced, sensitive, and non-publicly available information must be labeled as “Restricted Information”. Backups must not be stored on the same hardware device as the original information.

Target Implementation Date: April 2015.

Responsible Official: Manager, Corporate Information Security

This report and management’s response does not contain proprietary or sensitive business information that may be exempt from disclosure pursuant to the Freedom of Information Act.

Chuck McGann 2014.08.18
08:30:35 -04'00'

Chuck L. McGann
Manager, Corporate Information Security

cc: Kimberly F. Benoit
Deputy Assistant Inspector General for Information Technology & Data Analysis
Sally Haring, Manager, Corporate Audit and Response Management
John Edgar, VP, Information Technology
CARMManager@usps.gov
E-FOIA@uspsoig.gov