NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

SECURITY OF
THE NCUA DATA CENTER

Report # OIG-13-08

August 12, 2013

James Hagen
Inspector General

W. Marvin Stith, CISA
Senior IT Auditor

Table of Contents

Section	Page
EXECUTIVE SUMMARY	1
BACKGROUND	2
OBJECTIVE, SCOPE AND METHODOLOGY	4
RESULTS IN DETAIL	5
APPENDIX	
A. NCUA Management Comments	11

Executive Summary

We conducted an audit to determine whether NCUA has adequate controls in place to protect computer systems and data in the [redacted] data center (data center) and in the [redacted] computer rooms (computer rooms).

To accomplish this audit, we conducted fieldwork at NCUA's [redacted] [redacted], the disaster recovery data center in [redacted], [redacted] [redacted]. We interviewed management and staff from the NCUA Office of the Chief Information Officer (OCIO); Division of Procurement and Facilities Management (DPFM); and AMAC. We reviewed NCUA documentation pertaining to the security of NCUA applications and data. We also reviewed National Institutes of Standards and Technology policy and procedure publications.

We determined that overall the NCUA has controls in place to protect the computer systems and data hosted in its data center and in its computer rooms. However, NCUA could make improvements to more adequately control or monitor access to the data center's server room and control access to the computer rooms: Specifically, NCUA needs to:

- [redacted];
- [redacted];
- [redacted]
- [redacted].

We made four recommendations where NCUA could make improvements to better protect access to its mission critical applications and data. NCUA agreed with all our recommendations. NCUA also indicated that in addition to OCIO and AMAC working together to address the security issues, the Office of the Chief Financial Officer will help address recommendations 1, 2, and 4. We have included NCUA's comments in their entirety at Appendix A. We appreciate the courtesies and cooperation NCUA management and staff provided to us during this audit.

Background

Information Technology (IT) operations are a crucial aspect of most organizational operations, and agencies rely on their information systems for their operations. One of the main concerns is business continuity. If a system becomes unavailable, agency operations may be impaired or stopped completely. It is necessary to provide a reliable and secure infrastructure for IT operations, in order to minimize any chance of disruption.

Data centers run organizations. The role of a data center includes generating revenue, storing sensitive data, and providing business-critical services. Because of their criticality and value, they are targets. A data center has to offer a secure environment, which minimizes the chances of a security breach. Therefore, a data center must keep high standards for assuring the integrity and functionality of its hosted computer environment. A secure environment that minimizes the chance of a security breach and unauthorized access to an agency's information systems would help protect sensitive data and mitigate intentional disruption of business-critical services.

While threats to an agency's computer systems and data can come from insiders or outsiders, insiders have a significant advantage over others who might want to harm the agency. Agencies implement security mechanisms such as electronic building access systems primarily to defend against external threats. However, insiders are not only aware of their organization's policies, procedures, and technology, but they are often also aware of their vulnerabilities.

NCUA hosts the following systems that are critical to NCUA's mission:

- GSS (General Support System): Provides agency-wide network and computing infrastructure and is the computing platform for all major NCUA business applications.

- AIRES (Automated Integrated Regulatory Examination System): Enables NCUA and state examiners to review and validate financial data related to the operations of federally insured credit unions (FICUs) and some state-chartered, non-federally insured credit unions (NFICUs).

- ODCS (Call Reporting System): The primary means by which NCUA collects, validates stores and reports financial and operational data for all FICUs and some state-chartered NFICUs.

- IIS (Insurance Information System): Enables NCUA and member credit unions to update, submit, track and manage credit union master information.

- ALMS (Asset Liquidation Management System): Provides the computing platform for the accounting of credit unions involved in the process of liquidation and all major business applications of AMAC.

Objective, Scope and Methodology

The objective of this audit was to determine whether NCUA has adequate controls in place to protect computer systems and data in the [redacted] data center and in the [redacted] computer rooms.

To accomplish this audit, we conducted fieldwork at NCUA's [redacted], the disaster recovery center in [redacted], and the [redacted]. We interviewed management and staff from the NCUA Office of the Chief Information Officer (OCIO); Division of Procurement and Facilities Management (DPFM); and AMAC. We reviewed NCUA documentation pertaining to the security of NCUA applications and data. We also reviewed National Institutes of Standards and Technology policy and procedure publications.

We conducted this review from April 2013 through August 2013 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. During this audit, we used access authorization lists and access history logs generated from the [redacted][1] system. We did not test the automated internal controls of this system. We relied on interviews and what we learned about the operation of and NCUA's manual controls associated with this system.

[1] [redacted] operates and manages security systems for its clients.

Results in Detail

We determined that overall the NCUA has controls in place to protect the computer systems and data hosted in its [redacted] data center (data center) and [redacted] computer rooms (computer rooms). However, the NCUA could make improvements to more adequately control or monitor access to the data center and control access to the computer rooms: Specifically, NCUA needs to:

- [redacted];
- [redacted];
- Log visitor access to the data center; and
- [redacted].

NCUA Data Center Structure and Access

The following rooms comprise the [redacted] data center:

- [redacted] Systems Office – an administrative office area;
- Server room - houses the servers hosting [redacted] applications and data;
- Development lab - [redacted];
- File room - [redacted]; and
- Storage room - [redacted].

Below is generalized illustration of the data center:

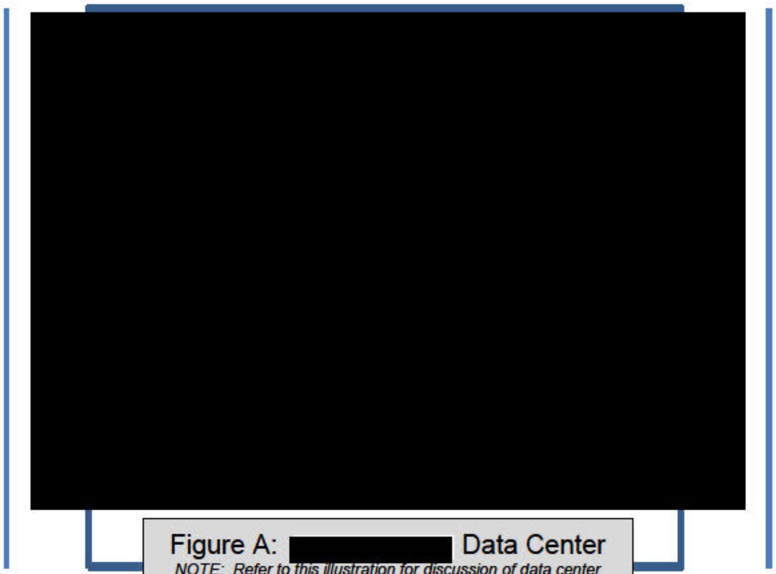

[redacted]

Figure A: [redacted] Data Center
NOTE: Refer to this illustration for discussion of data center doors in the body of the report.

NCUA employs the [redacted] system to monitor access to the [redacted] data center. The [redacted] of the data center include the server room, development lab, file room, and the storage room. A user requires a properly coded card to enter the data center, which creates an audit trail in the [redacted] system recording the card/user identity at the time of access. The [redacted] system monitors and records both authorized and unauthorized access events. Access logs can be read out at the [redacted] facility, and the NCUA Security Specialist can read the access logs at the [redacted] facility via a web interface with the [redacted] system. NCUA's Division of Procurement and Facilities Management (DPFM) enters into the [redacted] system users who are authorized to access secured areas.

As stated above, the server room hosts NCUA applications and data. Therefore, it is the most critical room in the data center. To access the server room, an authorized user[2] can either:

[redacted]

[redacted].

[2] [redacted]

NCUA Needs to Improve Security of the [redacted] in the Data Center's Server Room

The server room's [redacted] could potentially provide unauthorized access to the server room.

[redacted]. This would facilitate someone to gain unauthorized access directly into the server room and disrupt NCUA operations.

Recommendation 1: [redacted].

Management Response:

We concur. OCIO has plans to meet with NCUA's Data Center Manager in mid-August to discuss the data center layout and address [redacted] options. We expect to have a viable solution by the end of the third quarter 2013 with layout changes complete by December 2014.

OIG Response:

We concur with management's planned actions.

NCUA Needs to Improve Security between the Data Center's [redacted] and the Server Room

The structure of the data center's [redacted] could potentially provide unauthorized access into the data center's server room.

[redacted]

[3] [redacted]

[redacted].

We recognize that the data center has a layer of physical security [redacted]. However, this configuration is unconventional from a security control perspective in that [redacted]. Consequently, this configuration presents a peculiar and unnecessary point of weakness within the data center's layered security that could potentially facilitate unauthorized access into the server room. This could allow access to the servers containing NCUA applications and data and disruption of NCUA operations.

Recommendation 2: [redacted].

Management Response:

We agree [redacted]. OCIO is already scheduled to meet with the Data Center Manager and will develop a plan [redacted] by December 2014.

OIG Response:

We concur with management's planned actions.

NCUA Needs to Improve Visitor Access Control to the Data Center

NCUA has not consistently logged visitor access to the data center. In addition, NCUA's security policy for logging visitors into the data center is inconsistent with the method we observed NCUA has used for logging visitors.

OCIO keeps its visitor sign-in log [redacted]. However, there is evidence that OCIO does not consistently use the log. Specifically, we reviewed the log and determined it included entries from June 2005 through May 2013:

- There are 119 entries between September 2005 and October 2010 - an average of approximately two visits per month;

- There are 14 entries between January 2011 and November 2012 - approximately only one visit every two months;

- There was no entry on September 19, 2012 when contractors visited the data center as part of the 2012 FISMA review;[4]

- The OIG visit on May 17, 2013 - for a tour of the data center as part of this audit - was the first entry in the log since November 2012.

In addition, OCIO management and staff were not aware of the active use of a visitor log - they did not object to a finding during the 2012 FISMA review that indicated "NCUA does not maintain a log at the entrance of the data center to record data center visitors."

Furthermore, NCUA changed its security policy to reflect its intended new visitor logging procedure as follows: "The Data Center Manager is responsible for ensuring that physical access to the Data Center is logged into the System's Division Calendar located in SharePoint." However, the Director, Division of IT Operations, who has overall responsibility for the data center indicated OCIO does not use SharePoint for logging visitors into the data center.

Without adequate logging of visitors, an accurate audit trail would be more difficult to reconstruct in the event of an incident within the data center.

Recommendation 3: We recommend NCUA review, document, and implement current policy and procedures for logging visitor access to the data center.

Management Response:

We agree and will have OCIO work with the Data Center Manager to ensure compliance effective immediately.

OIG Response:

We concur with management's planned actions.

[4] We did not pursue whether or not there were other visitors to the data center during the period covered by the visitor's log that OCIO staff should have logged.

NCUA Needs to Improve Security of [redacted] Computer Rooms

The physical structures of the two computer rooms could allow for unauthorized access to the servers containing AMAC applications and data.

[redacted].

[redacted].
Consequently, a determined individual could gain access to the AMAC servers and disrupt AMAC operations.

Recommendation 4: [redacted].

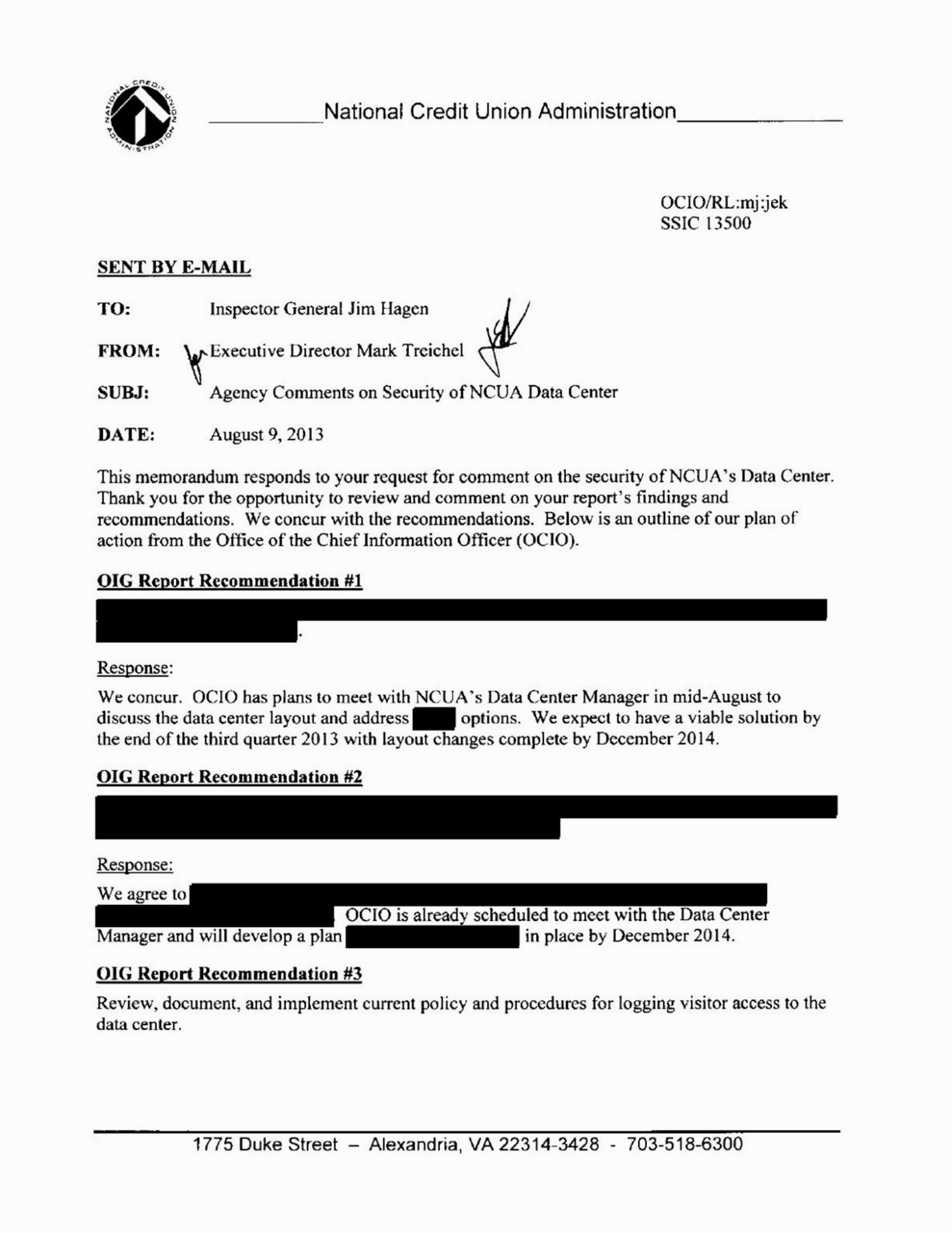
Management Response:

We agree that [redacted]. OCIO met with AMAC to discuss the Data Center in late July. OCIO and AMAC will work together [redacted] installed by December 2014.

OIG Response:

We concur with management's planned actions.

Appendix A - NCUA Management Comments



National Credit Union Administration

OCIO/RL:mj:jek
SSIC 13500

SENT BY E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Agency Comments on Security of NCUA Data Center

DATE: August 9, 2013

This memorandum responds to your request for comment on the security of NCUA's Data Center. Thank you for the opportunity to review and comment on your report's findings and recommendations. We concur with the recommendations. Below is an outline of our plan of action from the Office of the Chief Information Officer (OCIO).

OIG Report Recommendation #1

[redacted].

Response:

We concur. OCIO has plans to meet with NCUA's Data Center Manager in mid-August to discuss the data center layout and address [redacted] options. We expect to have a viable solution by the end of the third quarter 2013 with layout changes complete by December 2014.

OIG Report Recommendation #2

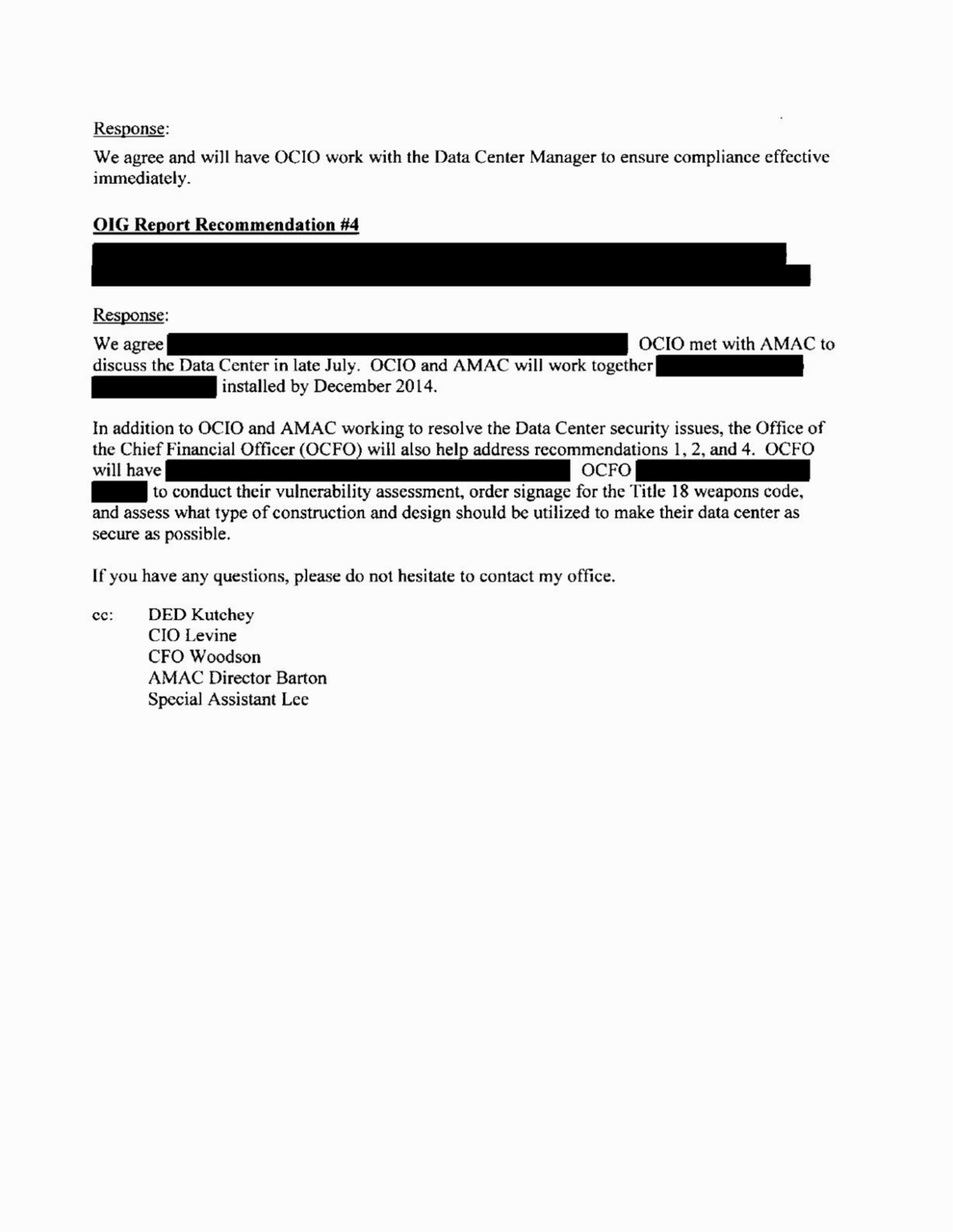
[redacted]

Response:

We agree to [redacted] OCIO is already scheduled to meet with the Data Center Manager and will develop a plan [redacted] in place by December 2014.

OIG Report Recommendation #3

Review, document, and implement current policy and procedures for logging visitor access to the data center.



Response:

We agree and will have OCIO work with the Data Center Manager to ensure compliance effective immediately.

OIG Report Recommendation #4

[redacted]

Response:

We agree [redacted] OCIO met with AMAC to discuss the Data Center in late July. OCIO and AMAC will work together [redacted] installed by December 2014.

In addition to OCIO and AMAC working to resolve the Data Center security issues, the Office of the Chief Financial Officer (OCFO) will also help address recommendations 1, 2, and 4. OCFO will have [redacted] OCFO [redacted] to conduct their vulnerability assessment, order signage for the Title 18 weapons code, and assess what type of construction and design should be utilized to make their data center as secure as possible.

If you have any questions, please do not hesitate to contact my office.

cc: DED Kutchey
CIO Levine
CFO Woodson
AMAC Director Barton
Special Assistant Lee