FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

Inspection of the Federal Election Commission's Kastle Key Program

December 2011

ASSIGNMENT No. OIG-11-02

OFFICE OF INSPECTOR GENERAL

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the Federal Election Commission (FEC), the Administrative Services Division (ASD) has oversight of the Kastle key program. The Kastle key program provides FEC employees and contractors with access to the main building entrance, FEC garage, elevators, and access to restricted offices (i.e. computer rooms, Finance Office). The Kastle program is governed by Commission Bulletin 2001-10: *Kastle Key Procedures,* and the Kastle Weblink System is used by ASD to manage the Kastle key data.

With the exception of the Office of General Counsel (OGC), and the Office of Compliance (Compliance), requests for Kastle keys are sent to the ASD Kastle key administrators from a FEC supervisor/manager for each FEC employee, or from the contracting officer technical representative (CoTR) or point of contact (POC) for contractors. For OGC and Compliance staff, requests for Kastle keys are made by the respective offices' administrative assistant; the administrative assistant contacts the Kastle key administrators to request keys for their office staff. Only the Kastle key administrators have the authority to access the Kastle Weblink System to activate, revoke (deactivate), or change Kastle key data. The Kastle key administrators are also able to view and export reports of Kastle data within the Kastle Weblink System.

The Office of Inspector General (OIG) conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspections and Evaluations*, January 2011. The OIG's objective for this inspection was to identify any management processes or controls concerning the FEC's Kastle key system that can be improved, and provide management with recommendations to help strengthen this FEC function. The OIG has identified three findings while conducting this inspection: **(1)** the Kastle key policy is outdated and does not reflect the current processes and procedures of the program, **(2)** the FEC is not in compliance with the current Kastle key policy, and **(3)** ASD needs to improve their process for monitoring the Kastle key program to address the control weaknesses identified during this inspection.

The significant issues identified during detailed testing that resulted in the three findings listed above include:

- The Kastle key policy has not been updated since 2001 and does not reflect the FEC's current processes;
- Supervisory approval for several FEC employees and contractors issued Kastle keys could not be located;
- 38 Kastle key users were listed as having more than one active Kastle key in their possession;
- Kastle key administrators are not revoking returned, lost, or broken keys prior to issuing new and/or replacement keys;
- Keys are issued to contractors with building access that was not authorized in accordance with the contract terms;
- Kastle keys are not consistently terminated for separated employees/contractors in a timely manner;

- Kastle keys located in inventory were still active and listed on the active users' report as assigned to Kastle users; and
- ASD does not have an adequate monitoring process established to properly manage the Kastle program.

With an outdated policy, an inadequate monitoring process, and weak program controls, the FEC is not in compliance with the Office of Management and Budget (OMB) Circular A-123: *Management's Responsibility for Internal Control* regarding the Kastle key program. OMB's Circular A-123 states "...*Federal managers must take systematic and proactive measures to… (ii) assess the adequacy of internal control in Federal programs and operations; [and] (iv) identify needed improvements*." However, the FEC has failed to implement a standard monitoring process that will assess the adequacy of internal controls or identify any necessary improvements for the FEC's Kastle key operations. In addition, ineffective internal controls exposes the FEC to a greater risk of providing unauthorized access to the FEC building, to include computer rooms that house expensive computer equipment and important agency data, and access to restricted offices that contain personally identifiable information (PII). Further, these weaknesses, if uncorrected, hinder ASD from preventing potential fraud and the ability to detect abuse of agency assets because the FEC is not exercising the proper controls to ensure Kastle key users are only provided with authorized access.

The OIG has proposed 15 recommendations to ASD to assist in addressing the identified findings and issues listed above. Management has agreed to implement 14 of the 15 recommendations.

BACKGROUND

The Federal Election Commission's (FEC) Administrative Services Division (ASD) manages the FEC's Kastle key program. Agency documentation shows that the FEC has contracted with Kastle Systems LLC (Kastle) for close to 20 years to provide building access. The Kastle keys provide FEC employees and contractors access to the FEC's main front entrance, garage, elevators, and restricted FEC offices. Kastle keys provide access to restricted offices and the FEC garage during normal business hours and full building access after normal business hours, Monday-Friday from 6pm to 6:30am. Kastle keys can also provide 24 hour access to the FEC building on the weekends. At the start of the OIG inspection, FEC was operating in their second option year of a 5 year contract with Kastle for fiscal year (FY) 2011. The average annual cost for the FEC's Kastle service is approximately $24,000.

When the FEC initially contracted with Kastle for building access, the program was centralized and all program tasks were managed by the ASD. The ASD was required to communicate with the vendor to activate and revoke (deactivate) keys, and make changes to the Kastle data. The initial policy that governed the Kastle program was Directive No. 55.

In 2001, Directive No. 55 was superseded with Commission Bulletin 2001-10: *Kastle Key Procedures*. Since then, changes have occurred to the Kastle program. The ASD manager and two ASD staff (Kastle key administrators) assist in managing the Kastle key program. The Kastle key administrators are now able to independently manage the FEC's Kastle data using the Kastle Weblink System. This system allows the Kastle key administrators to activate keys, enter in user key information (i.e. user name, key number, etc.), revoke keys, create reports of Kastle data, and view the daily key activity of users for the past 90 days. A Kastle key can be issued by the Kastle key administrators on a permanent basis or for temporary use. The Kastle key administrators are also able to place requested access restrictions on keys, such as Monday–Friday access only, restricted floor access, garage access, etc.

The Office of General Counsel (OGC) and the Office of Compliance (Compliance) have assumed administrative responsibilities for keys that are issued to their staff. In prior years when only ASD maintained Kastle keys, OGC and Compliance experienced frequent occurrences of keys not being activated prior to being issued to a user, and keys that were tested to ensure activation but then did not work on the day staff needed to enter the building. Due to these problems, OGC and Compliance keep an inventory of Kastle keys to distribute new, temporary, and replacement keys. Although physical keys are maintained by OGC and Compliance, these two offices are still required to contact the ASD Kastle key administrators to activate, revoke, or make any changes to their staff's key information.

According to policy, Kastle keys must be requested by a supervisor or manager for FEC staff. The supervisor should communicate the need for the key (i.e. access to computer room, garage, etc.) and the key is then activated accordingly by the Kastle key administrator and provided to the key user. In addition to FEC employees, FEC contractors are also able to receive Kastle keys to access the FEC building, garage, and other offices such as the Finance

Office that require Kastle key access. For keys requested for contractors that need to access the building after hours, the written contract terms must specify that the contractor is allowed to access the FEC building during non-business hours. The contracting officer's technical representative (CoTR) or point of contact (POC) for the contractor should request the Kastle key from the Kastle key administrators with the appropriate access identified by the contract terms.

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives
The Office of Inspector General's (OIG) objectives for conducting an inspection of the Federal Election Commission's (FEC) Kastle key program were to identify any management processes or controls concerning the FEC's Kastle key system that can be improved, and provide management with recommendations to help strengthen this FEC function.

Scope
The scope of the inspection included active Kastle key users as of August 4, 2011 and Kastle key daily activity data from May 2011 to August 2011.

Methodology – The OIG conducted the following inspection steps:

- Reviewed the Administrative Service Division's (ASD) policies and procedures for compliance and adequate management processes and controls.

- Interviewed the Office of General Counsel (OGC) and the Office of Compliance (Compliance) administrative assistants responsible for issuing keys to their respective offices.

- Verified if Kastle keys maintained by ASD, OGC, and Compliance were securely stored.

- Documented key numbers maintained as inventory for ASD, OGC, and Compliance to determine if the keys had all been properly revoked.

- Conducted a walkthrough with the ASD manager and Kastle key administrators to understand how a Kastle key is requested, issued, activated, tracked/monitored, and revoked (deactivated).

- Reviewed Kastle key data reports for current active users, revoked keys, and the daily Kastle activity report.

- Interviewed a FEC team representative from Kastle Systems LLC to gain a better understanding of the Kastle Weblink System used to manage the FEC's Kastle data.

- Conducted an employee survey to verify which keys were assigned and in the possession of Kastle users who are listed in the Kastle Weblink system as having multiple active keys.

- Conducted detailed testing to determine if:
  - ASD is revoking Kastle keys for separated FEC employees and/or contractors in a timely manner;
  - All persons listed on the active Kastle key report are current FEC employees or contractors; and contractors are provided the appropriate authorized access according to contract terms.

INSPECTION FINDINGS AND RECOMMENDATIONS

A. Kastle Key Policy Not Updated

The current policy that governs the Kastle key program is Commission Bulletin 2001-10: *Kastle Key Procedures*. Based on the Office of Inspector General's (OIG) review of the policy, and discussions with the Administrative Services Division (ASD), the policy has not been updated since 2001 and does not reflect the current processes used by the Kastle key administrators.

Since 2001, ASD has not updated the policy to reflect the current ASD staff who oversee the program, or to reflect that the Office of General Counsel (OGC) and the Office of Compliance (Compliance) maintain their own inventory of Kastle keys and distribute permanent, temporary, and replacement keys to their own staff. In addition, the policy also fails to document the approval and distribution procedures for Kastle key requests that are made for contractors who access the building during non-business hours and/or offices with restricted access.

Further, the policy does not provide the Kastle key administrators with internal procedures for managing the program. Due to a lack of internal procedures, the OIG identified several errors and inconsistencies in the Kastle key report data. Without standard internal procedures to govern the Kastle key program, ASD is lacking consistent and adequate processes to properly manage and monitor the program. The lack of internal procedures also reduces the likelihood that the Kastle program can efficiently and effectively function in the event of extended absences or separations of the Kastle administrators. Although the ASD manager has expressed to the OIG that the division is in the process of updating the current policy, these updates have not yet been fully developed and implemented.

Recommendation #1

The Kastle key policy should be updated as soon as possible to include:

- The titles of current ASD positions that manage the Kastle key program;
- Instructions for contractor requests for Kastle keys; and
- Any other program changes implemented as a result of this inspection.

Management Response:
Agree- ASD management was already in the process of drafting a revision to the outdated Kastle Key policy before OIG initiated the inspection. Revision efforts were put on hold pending the outcome, findings, and recommendations of this inspection.

OIG Comments:
The OIG believes management's response will address this recommendation once fully implemented. The OIG looks forward to reviewing the revised policy to ensure it fully addresses this recommendation.

Recommendation #2

Include guidelines and responsibilities for Kastle administrators and contractors needing Kastle keys.

Management Response:
Agree- Guidelines for issuing Kastle keys to contractors will be discussed with the Office of the Staff Director, to decide how this should be incorporated into the revised policy. A COTR or federal employee should be on site with contractors who are in the building after hours. In addition, it is the responsibility of the COTR to work with the Contracting Officer to ensure appropriate language is included and/or revised in contracts authorizing contractors to work after hours.

OIG Comments:
Although management agreed with the OIG's recommendation, the OIG believes that management's proposed action to have a CoTR or federal employee on site with contractors who access the building after hours is not practical or feasible for all contracting situations. The OIG believes the following current controls, if properly monitored, are reasonable to address contractor after hour access: security clearances provided by the Office of Personnel Management for contractor background checks; ensuring the Contracting Officer has verified contractors have the authority to access the FEC building after hours; and ASD providing the appropriate building access and/or restrictions according to the contract terms.

Recommendation #3

Document the procedures that ASD staff must follow when recording Kastle key data in the Kastle Weblink System.

Management Response:
Agree- ASD will establish a standard format for entering data (required fields) into the Kastle system to ensure information is consistent when reflected on reports. This will only apply to new or edited data in the Kastle system.

OIG Comments:
Although management has generally agreed with the OIG's recommendation, ASD has only agreed to follow standard procedures for new Kastle key requests or for current data that requires edits. The OIG believes that ASD should be consistent and ensure that all data (current data and new data) in the Kastle Weblink system aligns with the new standards once implemented. The OIG believes only if <u>all</u> data is

revised according to the new standard procedures will this recommendation be fully implemented.

Recommendation #4

The updated policy should require that requests for and approvals of Kastle keys should be in writing and approvals should be maintained by ASD.

Management Response:
Agree- "In writing" requests will be accepted via electronic or hardcopy format. Current ASD management is not responsible for missing/inaccurate kastle key request/approval records that were granted or obtained prior to March 2011.

OIG Comments:
The OIG believes management's response will address this recommendation when fully implemented.

Recommendation #5

ASD should consider creating a request form for supervisors, managers, contracting officer's technical representatives (CoTRs), and points of contacts (POCs) to complete when requesting a Kastle key for an employee or contractor. The required information on the form should include (but not limited to):

- date requested;
- key user's full name;
- identification of the requesting department/division;
- identification if an employee or contractor;
- expiration date (temporary keys);
- access restrictions or additions (i.e. garage, specific floors, etc.);
- signature of approval from supervisors and/or managers for FEC employees to access the FEC building during non-working hours; and
- signature of CoTR (when applicable for contractors) verifying contract includes the need to have access during non-business hours.

Management Response:
Agree- The idea for using a standardized format, such as a form, of information an individual is required to provide to request a Kastle key was originally proposed by current ASD management and discussed during one of the OIG inspection meetings. Request form may be created in email format or hardcopy. Signatures may be substituted with an electronic signature, or "X" mark for verification of certain information.

OIG Comments:
The OIG believes management's response will address this recommendation when fully implemented.

Recommendation #6

Ensure users are aware of all available services and contact information for Kastle Systems LLC when issues occur with their physical key that prevents access to the FEC building.

Management Response:
Disagree- When ASD management contacted a Kastle key representative from our Kastle Team to inquire about the hotline service, the representative was not aware of such a service and/or any parameters for granting access. ASD management needs to do further research and speak with the individual the OIG contacted at Kastle to verify how this hotline works and if enough information is being gathered by Kastle representatives to validate a person's identity before allowing access to the building. The information OIG provided on how the hotline works, was not sufficient to make a final determination on if this service should be advertised and whether or not the information gathered by Kastle during the call is an adequate security protocol measure for identity verification and granting remote access.

OIG Comment:
As previously discussed, the OIG gained our information regarding this service by calling the service number identified in the current policy (Commission Bulletin 2001-10) and speaking with a Kastle System representative who provides the service. The OIG believes providing the Kastle contact information and procedures that can grant emergency access for approved Kastle users is an important and useful customer service tool. This service will be helpful for those users who may experience key errors when trying to enter the building on the weekends or need to access the building after normal business hours. However, the OIG agrees that management should conduct further research regarding this service and verify if sufficient and adequate information is required by Kastle prior to granting building access.

B. Non-Compliance with Agency Kastle Key Policy

The ASD is not in compliance with the current Kastle key policy. The Kastle key administrators' process for assigning, activating, and revoking Kastle keys is not performed in accordance with the policy's procedures. The Kastle key policy indicates that Commission Bulletin 2001-10 was implemented "…*to control the assignment of new insert keys*…" However, OGC and Compliance distribute Kastle keys to their staff and these keys are not properly controlled or managed by ASD. The OIG identified keys maintained by OGC and Compliance that were located in inventory but also listed as active on the Kastle key data report. In addition, the documentation maintained by OGC and Compliance was not kept up to date to reflect current employees issued Kastle keys or the correct keys that were assigned. Dates recorded by OGC and Compliance for temporary keys did not always match the Kastle Weblink System data, and Compliance was unable to locate Kastle keys that were provided to them by ASD. The lack of control over the keys issued by OGC and Compliance increases the risk that Kastle keys are not revoked in a timely manner, inaccurate data is stored in the Kastle Weblink System, and employees and/or contractors are granted building access beyond the authorized time period for temporary keys.

ASD also does not consistently maintain sufficient evidence of supervisory approval for the issuance of Kastle keys, or evidence that Kastle key users signed for the key acknowledging receipt of a Kastle key. Based on detailed testing of a sample of 15 Kastle key users, the OIG identified that:

- For 6 out of the 15 Kastle keys assigned, there was no documentation of supervisory approval; and
- For 9 out of 15 Kastle key users, there was no evidence to verify the user signed for the receipt of a Kastle key.

Also, keys are not consistently returned and/or immediately revoked for separated employees and contractors. In addition, Kastle key administrators fail to immediately revoke keys that are lost or broken. According to Commission Bulletin 2001-10, ASD's policy is to immediately revoke Kastle keys; however, contrary to the policy, keys that are returned, lost, or broken are often not revoked by the Kastle key administrators, but left as active in the Kastle Weblink System and re-assigned to another user.

Recommendation #7

> The management functions of the Kastle key program should be centralized and managed by the Administrative Services Division (ASD) only, to include the storage, assignment, distribution, activation, and deactivation of all Kastle keys.
>
> **Management Response:**
> Agree-this [current] procedure was implemented at some point by previous management. Current management agrees that the Kastle key program should be soley managed by ASD. Prior to the OIG audit, ASD management requested OGC

and Office of Compliance offices provide updated and accurate information on individuals within their group who were issued Kastle keys and reminded them of the importance of providing timely updates to the ASD when keys were handed out or returned. ASD is currently the only office that is able to activate and deactivate Kastle keys in the Kastle system as outlined in the current policy.

OIG Comments:
The OIG believes management's response to have the Kastle key program solely managed by ASD, to include the issuance of Kastle keys to all FEC staff and contractors will address this recommendation when fully implemented.

Recommendation #8

The ASD should maintain a record of Kastle key requests by supervisors, managers, contracting officer's technical representatives (CoTRs), and contract point of contacts (POCs).

Management Response:
Agree- the current policy, however, does not indicate that ASD must maintain a record of this information after received, nor does it indicate how long such records should be maintained. In addition, employees who park in the garage are required to have a Kastle key for access; in this case, supervisory approval is not necessary and would not be required for issuance.

OIG Comment:
Management has agreed with the recommendation, and the OIG believes once fully implemented, the recommendation will be addressed. ASD should follow records management procedures for maintaining documentation of Kastle key requests.

Recommendation #9

The ASD should require a signature of receipt from Kastle users for all assignments of permanent and temporary keys in accordance with FEC policy.

Management Response:
Agree- some type of signature receipt or log will be maintained when Kastle keys are issued and the new process will be included in the revised policy.

OIG Comment:
The OIG believes management's response will address the recommendation once fully implemented.

Recommendation #10

The ASD should notify the Kastle users of the Kastle key policy and user responsibilities when keys are issued (for example, provide policy, require signature of understanding and compliance with policies and procedures, and post the policy in a convenient place for users to access [i.e. FECNet, the FEC's Intranet site]).

Management Response:
Agree- ASD management will examine options for providing this information.

OIG Comment:
The OIG believes management's response will address the recommendation once fully implemented.

Recommendation #11

The ASD should work with the FSA (FEC System Access) team to ensure that the Kastle key administrators receive email notification when employees and contractors are separated from the FEC through FSA to ensure that Kastle keys are returned.

Management Response:
Agree- ASD will work with FSA team to ensure we are receiving email notifications for ALL employee and departures that are entered into FSA. FSA is currently our only source of notification for receiving termination/departure dates of employees/contractors.

OIG Comment:
The OIG believes management's response will address the recommendation once fully implemented.

C. Monitoring of the Kastle Key System Needs Improvement

Due to the hiring of a new ASD manager in early 2011, the Kastle key administrators conducted a review of Kastle keys in March 2011 to document all FEC employees and contractors who were currently issued a Kastle key and to remove active keys that were no longer in use. During the inspection, the OIG identified that the review conducted in March 2011 was not completed and the inaccurate data identified by the Kastle key administrators had not been corrected in the Kastle Weblink system. Through detailed testing, the OIG also identified that ASD lacks effective monitoring controls over the Kastle key program and does not have a formal review process or standard monitoring procedures to: (1) identify data that is inaccurate; (2) detect unusual Kastle key activity; or (3) monitor for data that should be changed or purged in the system to maintain accurate and current Kastle data.

The results of the OIG's testing revealed:

- employees and contractors who were no longer employed at the FEC had Kastle keys active in the Kastle Weblink System;
- Kastle key administrators failed to revoke lost, broken and returned keys prior to issuing new and replacement keys to users; and
- 38 individuals were listed in the Kastle Weblink System as having more than one active key, totaling 81 keys.

Further, the OIG verified through a survey that 39 of the 81 keys identified above were not in the possession of the users, and the 39 keys were also not found in the physical inventory of Kastle keys. Although the 39 keys were listed as active in the Kastle Weblink System, the OIG verified that the keys had no activity during the current 90 day recording cycle of daily activity for the scope of this inspection. Due to the inability to locate the physical keys, the OIG believes the 39 keys are prior keys that were issued to the users but have since been lost or broken and discarded by ASD; however, the Kastle key administrators have not removed the key data from the Kastle Weblink system.

In addition, the OIG identified 117 keys listed on the revoked Kastle key report as unassigned since April 2007; however, only 6 of the keys were actually located in ASD's physical key inventory. Further, 118 keys listed on the revoked list as "stock" (inventory) are not included in ASD's physical inventory of keys. The OIG also identified 73 keys that were revoked in 2007 and listed as broken or lost on the revoked Kastle key report but never purged from the Kastle Weblink System.

Recommendation #12

The ASD should implement a formal on-going monitoring process to verify that only current employees/contractors have active Kastle keys, and that users do not have more than one active Kastle key at a time.

Management Response:
Agree- ASD does not currently receive ongoing personnel information on active employees/contractors or effective terminations/separation dates for employees/contractors. This lack of resources hinders our ability to maintain and implement a formal, standard, ongoing monitoring process to verify holders of active kastle keys against an active employee/contractor list. If we are able to receive this information on an on-going basis from the appropriate department, we can implement the recommended controls. During the course of this inspection, ASD already began identifying users who have more than one active Kastle key, and have revoked any duplicate keys as appropriate.

OIG Comment:
In addition to management's plans, the OIG would suggest ASD review available FEC reports to verify current and terminated FEC employees. For instance, ASD can

review the Office of Human Resource's list of persons who hire on and separate from the agency and the FEC's staffing report of all current employees. These reports can be used as verification documents in addition to working with the FSA team to receive email notifications regarding the status of employees and contractors. The OIG believes management's response will address this recommendation once fully implemented.

Recommendation #13

ASD should require that all requests for temporary keys include an expiration date. The monitoring process implemented should include procedures for ensuring temporary keys are properly tracked, revoked timely, and that the system properly reflects the current person using the key.

Management Response:
Agree-requiring an expiration date for temporary keys can be addressed in the revised policy.

OIG Comment:
The OIG believes management's response will address this recommendation once fully implemented. The OIG looks forward to reviewing the revised policy to ensure this recommendation has been fully addressed.

Recommendation #14

ASD should implement a formal annual review process for periodically reviewing and cleaning up Kastle data reports. Any revoked Kastle keys that are no longer physically in stock, broken/inoperable, or lost should be removed from the system after these keys have been inactive for a certain period of time (e.g. one year).

Management Response:
Agree- ASD can work with Kastle Systems on identifying the best process for deleting revoked keys not physically in stock from the Kastle System. ASD did not previously have the ability to delete such keys from the system directly; this may be an added feature in the new system. Though revoked keys cannot be used to access the building after hours, if stale data can be removed from the system, it will allow for more efficient management of the Kastle key inventory.

OIG Comment:
The OIG believes management's response will address this recommendation once fully implemented.

Recommendation #15

All Kastle key numbers included on the revoked list that are not currently in stock and have had no activity since 4/25/2007 should be deleted from the Kastle system.

Management Response:
Agree- ASD can work with Kastle Systems on identifying the best process for deleting revoked keys not physically in stock from the Kastle System. ASD did not previously have the ability to delete such keys from the system directly; this may be an added feature in the new system. Though revoked keys cannot be used to access the building after hours, if stale data can be removed from the system, it will allow for more efficient management of the Kastle key inventory.

OIG Comment:
The OIG believes management's response will address this recommendation once fully implemented.

CONCLUSIONS

The Federal Election Commission (FEC) is at an increased risk of providing unauthorized access to FEC employees and contractors due to inadequate controls over the Kastle key program. Failure to establish and implement proper controls to ensure only current FEC employees and contractors have active Kastle keys, and that building access has been approved and properly assigned, exposes the FEC to potential fraud and abuse. Since the Kastle keys grant access to areas such as the FEC computer rooms and access restricted offices that contain personally identifiable information (PII), it is imperative that the Administrative Services Division (ASD) have processes and procedures in place to ensure only those persons who are properly authorized has access to those areas of the building.

According to the Office of Management and Budget's (OMB) Circular A-123: Management's Responsibility for Internal Control:

> *"Agencies and individual Federal managers must take systematic and proactive measures to … (ii) assess the adequacy of internal control in Federal programs and operations; … (iv) identify needed improvements;[and] (v) take corresponding corrective action; …"*

The Office of Inspector General (OIG) believes that frequent turnover in the ASD manager position has hindered the ASD from complying with OMB's guidance in establishing proper internal controls for the Kastle key program. From summer 2008 to January 2011 alone, ASD has hired two permanent staff in the ASD manager position and shortly thereafter, both hired staff separated from the agency. In addition, the ASD had an acting ASD manager for almost one year, but was also responsible for other FEC managerial duties. The lack of consistent governance over the Kastle key program has contributed to a lack of program knowledge, controls, and continuous program monitoring.

Since the recent hire of the current ASD manager, ASD has made efforts to improve the Kastle key program with the initial Kastle key review in March 2011, and the ASD manager's effort to begin developing preliminary changes and updates to the current policy. The OIG acknowledges these efforts; however, much progress is still required in order for the FEC to obtain an efficient and effective Kastle key program. The OIG believes implementation of the recommendations provided in this inspection report will assist ASD in establishing adequate controls, effective monitoring processes, and reduce the risk of the agency providing unauthorized access by ensuring building access is properly provided to FEC employees and contractors.

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

or toll free at 1-800-424-9530 (press 0; then dial 1015)
Fax us at 202-501-8134 or e-mail us at oig@fec.gov
Visit or write to us at 999 E Street, N.W., Suite 940, Washington DC 20463

Individuals including FEC and FEC contractor employees are encouraged to alert the OIG to fraud, waste, abuse, and mismanagement of agency programs and operations. Individuals who contact the OIG can remain anonymous. However, persons who report allegations are encouraged to provide their contact information in the event additional questions arise as the OIG evaluates the allegations. Allegations with limited details or merit may be held in abeyance until further specific details are reported or obtained. Pursuant to the Inspector General Act of 1978, as amended, the Inspector General will not disclose the identity of an individual who provides information without the consent of that individual, unless the Inspector General determines that such disclosure is unavoidable during the course of an investigation. To learn more about the OIG, visit our Website at: http://www.fec.gov/fecig/fecig.shtml

Together we can make a difference.