



governmentattic.org

"Rummaging in the government's attic"

Description of document: Closing documents from fifteen (15) specific Federal Election Commission (FEC) Office of Inspector General (OIG) investigations, 2008-2015

Requested date: 29-February-2016

Released date: 11-May-2016
2nd/final release date: 01-August-2016

Posted date: 16-July-2016
Update posted date: 22-August-2016

Note: Material released 01-August-2016 begins on PDF page 293

Source of document: Federal Election Commission
Attn: FOIA Requester Service Center
Room 408
999 E Street, NW
Washington, DC 20463
Fax: (202) 219-1043
Email: FOIA@fec.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: FOIA@fec.gov
Date: May 11, 2016 5:50:06 PM
Subject: Your Freedom of Information Act Request to the Federal Election Commission (FOIA 2016-32)

VIA ELECTRONIC MAIL

Re: Your FOIA Request to the Federal Election Commission 2016-32

This letter serves as the Federal Election Commission's (FEC) response and first document production to your request for information from the FEC under the Freedom of Information Act (FOIA), dated February 29, 2016 and received by the FEC's FOIA Requester Service Center the same day. You requested the following:

Copies of the final report, report of investigation, closing memo, referral memo, referral letter, and "any other conclusory" documents associated with the following closed Office of the Inspector General (OIG) investigations:

INV-08-01	INV-10-02	INV-13-04
INV-08-02	INV-11-01	INV-14-01
INV-09-01	INV-13-01	INV-14-02
INV-09-02	INV-13-02	INV-15-01
INV-10-01	INV-13-03	INV-15-02

We have searched the agency's records and located responsive documents related to INV-08-01, INV-09-01, INV-09-02, INV-10-01, INV-10-02, INV-11-01 and INV-13-04. See attached. As to INV-08-02, the FEC was unable to locate any responsive records. The FEC's OIG has indicated the other investigations as to which you have request records remain open. From the attached responsive documents we have redacted certain information pursuant to FOIA Exemptions 3(A), 5, 6, 7(C), and 7(D).

Exemption 3(A) prevents disclosure of information "specifically exempted from disclosure by statute (other than section 552b of this title), if that statute — (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3)(A). Pursuant to Section 7 of the Inspector General Act of 1978, the FEC is prohibited from disclosing the identity of an employee without the consent of the employee, after receipt of a complaint. 5 U.S.C. app. § 7(b). FOIA Exemption 5 protects from disclosure "inter-or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency," including documents covered by the attorney work-product, deliberative process, and attorney-client privileges. 5 U.S.C. § 552(b)(5). Exemption 6 protects from disclosure information that if released would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6). Exemption 7(C) protects from disclosure records or information compiled for law enforcement purposes that, if released, could reasonably be expected to constitute an

unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(7)(C). Exemption 7(D) provides protection for "records or information compiled for law enforcement purposes [which] could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source." 5 U.S.C. § 552(b)(7)(D).

We are continuing to process additional documents responsive to your request and will release those documents to you as soon as possible. Certain records responsive to your request contain information submitted to the FEC by a contractor that may be confidential commercial information. Pursuant to Executive Order 12,600, the Agency is required to give notification to those who submit business information to the government when that information becomes the subject of a FOIA request. See E.O. 12,600, 52 Fed. Reg. 23781 (1987). Accordingly, the Agency must provide the contractor with a pre-disclosure notification and a reasonable period of time in which to object to the disclosure of any of the requested material before any such material can be released. Additionally, other records responsive to your request include information pertaining to another federal agency. Thus, consistent with FOIA guidelines, these records require consultation with the other federal agency prior to release.

We anticipate that documents provided in the subsequent document production(s) may also have information redacted pursuant to Exemptions 3(A), 5, 6, 7(C), and 7(D), as well as Exemption 4. Exemption 4 protects from disclosure commercial and financial information that is privileged or confidential. 5 U.S.C. § 552(b)(4). In the letter accompanying the final document production, we will provide you with a list of all FOIA exemptions that have been applied to the records released and to the responsive records withheld in their entirety, as well as approximate page counts for the documents withheld pursuant to each FOIA exemption.

You may appeal any adverse FOIA determination. Any such appeal must be filed in writing and should follow the guidelines set forth in 11 C.F.R. § 4.8. If you have any questions, please contact the FOIA Service Center at FOIA@fec.gov, or (202) 694-1650.

Sincerely,

Peter K. Han
FOIA Requester Service Center



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CLOSING MEMORANDUM

Case #: INV-08-01	Prepared By: Joseph Duncan
Case Title: [REDACTED]	
Date of Report: 05/06/10	
Subject: Allegations of Misconduct	

From July 2008, thru January 2010, the OIG received twenty six (26) allegations of wrongdoing against [REDACTED], the former [REDACTED]. These allegations were made in eight (8) separate complaints. The OIG conducted investigations on three (3) of the 26 allegations and consolidated the investigative findings in this single Report of Investigation. These three investigations involved: 1) improper receipt of transit benefits; 2) reprisal for filing an OIG complaint; and 3) improper setting of senior level (SL) pay.

Alleged Improper Receipt of Transit Benefits

The transit benefit investigation was initiated following a complaint on July 23, 2008, which contained an allegation that [REDACTED] was parking in the FEC garage and, at the same time, collecting transit benefits, in violation of Commission Directive No. 54. This allegation was substantiated. The investigation found that [REDACTED] received FEC-paid parking and transit subsidy benefits during the months of April thru July of 2008. The investigation found that during the months of May, June, and July of 2008, [REDACTED] collected full transit benefits, but did not commute on public transportation for more than 50% of the business days in these months. Based on these findings, the OIG concluded that [REDACTED] did not comply with requirements under Commission Directive 54.

Alleged Reprisal for Filing an OIG Complaint

The reprisal investigation was initiated after [REDACTED], the former [REDACTED] filed a complaint on [REDACTED], 2008, alleging that [REDACTED] retaliated against [REDACTED], because [REDACTED] had [REDACTED]. The alleged acts of reprisal consisted of: 1) [REDACTED]; 2) [REDACTED]; and 3) [REDACTED]. The alleged reprisal was unsubstantiated. The investigation found no

evidence indicating that [REDACTED] knew about [REDACTED] [REDACTED] [REDACTED]. Furthermore, investigative findings did not support [REDACTED] claim that [REDACTED] [REDACTED], in retaliation for [REDACTED] protected disclosure.

Alleged Improper Setting of Senior Level Pay

On August 28, 2008, the OIG received a complaint alleging that [REDACTED] set [REDACTED] own pay, without Commission approval, after the Commission voted to appoint [REDACTED] in the position of Acting [REDACTED]. The investigation did not substantiate this allegation. The investigation found that Commissioner [REDACTED], who was the FEC Chairman at the time, approved the salary amount set, in connection with [REDACTED] [REDACTED] temporary senior level appointment. A review of Commission voting documents revealed that none of the Commissioners objected to the omission of [REDACTED]'s salary information on the voting documents, at the time the Commission voted on [REDACTED]'s appointment. Based on Chairman [REDACTED]'s approval, and no Commission objections to the salary omission, this allegation was unsubstantiated.

OIG Disposition: As a result of the OIG investigation, [REDACTED] repaid transit subsidies to the FEC in the amount of \$210. [REDACTED] resigned from the FEC in [REDACTED], unrelated to this investigation. On May 4, 2010, the OIG issued a Report of Investigation to the Commission. On that same day, the OIG referred the remaining 23 allegations to the Staff Director, due to the concerns raised in the allegations. These remaining allegations involved mostly hiring decisions, position upgrades, and promotions. Based on these activities, this investigation will be closed.

Concurrence: _____
Jon Hatfield, Deputy Inspector General Date

FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL



Report of Investigation

The Former Director of [REDACTED]

Case Number INV-08-01

May 4, 2010

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

TABLE OF CONTENTS

	<u>Page</u>
I. EXECUTIVE SUMMARY	1
II. BACKGROUND	2
III. ALLEGATIONS AND INVESTIGATION DETAILS	3
A. <u>Alleged Improper Receipt of Transit Benefits</u> ██████████ parked in the FEC garage, while ██████ participated in the transit benefit program, in violation of Commission Directive No. 54.	
B. <u>Alleged Reprisal for Filing an OIG Complaint</u> ██████████ retaliated against ████████████████████ for filing an OIG complaint.	
C. <u>Alleged Improper Setting of Senior Level Pay</u> ██████████ set his own salary when he was appointed to Acting ████████████████████, in violation of FEC Personnel Instruction 319.1.	
IV. FINDINGS AND CONCLUSION	9
V. PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE	9
ATTACHMENT	10
Summary of 26 allegations made against ████████████████████ submitted to the OIG in eight (8) separate complaints between July 23, 2008, and January 26, 2010	

I. EXECUTIVE SUMMARY

From July 23, 2008, thru January 26, 2010, the Office of Inspector General (OIG) received twenty six (26) allegations of wrongdoing against [REDACTED], the former Director of [REDACTED]. These allegations were made in eight (8) separate complaints. Based on the OIG's *Guidelines for Evaluating Hotline Complaints*, the following three (3) of the 26 allegations were investigated: 1) improper receipt of transit benefits; 2) reprisal for filing an OIG complaint; and 3) improper setting of senior level pay.

The remaining 23 allegations are being referred to management based on several factors and criteria established in the OIG's *Guidelines for Evaluating Hotline Complaints*. These allegations involved hiring decisions, position upgrades, promotions, and other matters. [REDACTED] resigned from the FEC in [REDACTED]. Since this investigation was concluded in April 2010, the OIG is reporting the investigative results to the Commission for information purposes. This investigative report makes no recommendations related to [REDACTED].

A. Alleged Improper Receipt of Transit Benefits

The transit benefits investigation was initiated following a complaint on July 23, 2008, which alleged that [REDACTED] was parking in the FEC garage and, at the same time, collecting transit benefits, in violation of Commission Directive No. 54. This allegation was substantiated. Commission Directive 54 prohibits employees who receive a "Federal parking benefit" from participating in the transit benefit program. The OIG investigation found that in April, May, June, and July of 2008, [REDACTED] received both transit benefits and federal parking benefits. When [REDACTED] was interviewed by the OIG, [REDACTED] acknowledged that [REDACTED] did not comply with the requirements under FEC Directive 54. [REDACTED] wrote a check in the amount of \$210, to reimburse the FEC for ineligible transit benefits [REDACTED] received.

B. Alleged Reprisal for Filing an OIG Complaint

The reprisal investigation was initiated after [REDACTED], the former [REDACTED], made allegations on August 25, 2008, that [REDACTED] retaliated against [REDACTED], because of a complaint [REDACTED] had previously filed with the OIG. [REDACTED] previously made a protected disclosure to the OIG. The investigative findings did not substantiate this allegation of reprisal.

alleged the following three acts of retaliation: 1) [REDACTED]; 2) [REDACTED]; and 3) [REDACTED]. The investigation found no evidence indicating that [REDACTED] knew about [REDACTED]'s prior complaint to the OIG. Furthermore, the findings did not support [REDACTED]'s claim that [REDACTED] [REDACTED], in retaliation for [REDACTED] protected disclosure.

C. Alleged Improper Setting of Senior Level Pay

On August 28, 2008, the OIG received a complaint alleging that [REDACTED] set his own pay, without Commission approval, after the Commission voted to appoint [REDACTED] to the Acting [REDACTED] position. The investigation did not substantiate this allegation of improper pay setting. The investigation found that Commissioner [REDACTED], the FEC Chairman at the time, gave approval for the salary amount that was set, in connection with [REDACTED]'s temporary appointment. A review of Commission voting documents revealed that none of the Commissioners objected to [REDACTED]'s salary information being omitted from the voting documents, at the time the Commission voted on [REDACTED]'s appointment. Based on Chairman [REDACTED]'s approval, and no Commission objections to the salary omission, the investigation did not substantiate this allegation.

II. BACKGROUND

The OIG evaluates each complaint it receives in accordance with the OIG's *Guidelines for Evaluating Hotline Complaints*. Under established guidelines, the OIG considers many factors in deciding whether to initiate an investigation based on a hotline complaint. The OIG reviews, evaluates, and make decisions on hotline complaints, based on the merits of the allegation, existing priorities, commitments, and resources.

It is acknowledged that not every allegation or complaint received can be investigated. Resource considerations when deciding whether to initiate an investigation may include current staffing levels and workloads. Evidentiary considerations may include the credibility of witnesses, the nature of the violation, the available evidence, the elements of required proof, and known mitigating circumstances.

The OIG received twenty six (26) allegations made against [REDACTED] during the period of July 2008, thru January 2010 (Attachment). Some of the allegations were repeated in more than one of the eight separate complaints with the OIG. Based on OIG guidelines, three (3) allegations were investigated. The remaining twenty three (23) allegations will be referred to management.

III. ALLEGATIONS AND INVESTIGATION DETAILS

A. Alleged Improper Receipt of Transit Benefits

Allegation 1: ██████████ parked in the FEC garage, while ██████ participated in the transit benefit program, in violation of Commission Directive No. 54.

On July 23, 2008, the OIG received a complaint alleging that ██████████ was parking in the FEC garage, while participating in the transit subsidy benefit program. According to the complainant, who requested confidentiality, in April 2008, ██████████ signed out a temporary FEC parking pass from ██████████, ██████████, Office of Administrative Services, to park ██████ black Lexus in the FEC garage. The complainant advised the OIG that ██████████ originally obtained the parking permit for ad hoc use, but then retained it, and continued to use it. The complainant further advised that ██████████ did not qualify for an FEC-paid parking pass, because he participated in the transit benefit program. The OIG initiated an investigation to determine if ██████████ violated FEC Directive No. 54.

FEC Commission Directive No. 54

FEC Commission Directive No. 54, “Employee Transit Benefit Program,” prohibits employees who receive a “Federal parking benefit” from participating in the transit benefit program. According to the Directive, a “Federal parking benefit” provides an employee with vehicle parking at a cost lower than local prevailing commercial parking rates. To be eligible for transit subsidy benefits, an employee must “regularly” commute via public transportation. For the purposes of this program, “regularly commute” means that *“the employee commutes via public transportation on a regular and recurring basis.”* To receive transit benefits, the Directive requires that public transportation be used *“a minimum of 50% of the available number of commuting days (business days) per month...”*

Under Commission Directive 54, if an employee regularly commutes to the FEC office using public transportation, but for whatever reason, does not commute on public transportation for more than 50% of the business days in a given month,¹ then they are only entitled to receive one-half (50%) of their full transit benefit for that month, rounded up to the next five dollar increment.²

¹ There are approximately 20 business days each month, so 10 business days would represent 50% of the total business days each month.

² If an FEC employee receives transit subsidy benefits of \$115 each month, but for whatever reason, will **not** commute to work 50% of the business days in a particular month; then the employee is only entitled to receive \$60 in subsidy benefits ($\$115 \times .5 = \57.50 , rounded up to \$60).

Under Commission Directive 54, it is the employees' responsibility to elect the correct subsidy amount each month (either the full amount or 50% of the transit benefit). This election amount should be based on the employee's anticipated use of public transportation during the next month; or based on the employee's actual use of public transportation during the previous month.

██████████ Receipt of Transit Benefits

The OIG obtained transactional activity records on ██████████'s SmarTrip card account (#██████████) from the Washington Metropolitan Area Transit Authority (WMATA). These records showed transit subsidy deposits, Metro station entries and exits, and parking, for the period of April 1, 2008, thru July 30, 2008. ██████████'s SmarTrip card activity showed that from April thru July 2008, ██████████ received transit subsidy deposits totaling \$460. Transit subsidy payments of \$115 were deposited into ██████████'s SmarTrip account on April 8th, May 6th, June 4th, and July 19th of 2008. The WMATA activity report further showed that ██████████ commuted by public Metro to work on 16 business days in April 2008; 7 business days in May 2008; one business day in June 2008; and 6 business days in July 2008.

██████████'s Receipt of FEC Parking Benefits

The OIG obtained a Kastle Systems key-card activity report on ██████████'s Kastle key-card #██████████. This Kastle report showed ██████████'s key-card, including garage and FEC building access entries and exits, for the period of May 1, 2008, thru July 30, 2008. According to the Kastle report, ██████████ accessed garage parking for his automobile 10 business days in May of 2008; 14 business days in June of 2008; and 17 business days in July of 2008.

██████████'s Interview

The OIG interviewed ██████████ on September 8, 2008, regarding his simultaneous receipt of FEC-paid parking benefit and transit subsidy benefits. In response to questions, ██████████ advised:

██████████ acknowledged that ██████████ drove to work and parked in the garage; while at the same time, ██████████ received benefits under the transit subsidy program. Around April 2008, ██████████ began driving to work on occasion because ██████████ was putting in long hours. Driving gave ██████████ more flexibility because ██████████ coached a ██████████ during the week.

██████████, the former ██████████, knew that ██████████ was working long hours and told him to go see ██████████, ██████████, about getting a temporary parking pass for the FEC building garage. ██████████ provided ██████████ a temporary parking pass that showed an expiration date of September 2008.

At the time ██████████ accepted the garage parking pass, ██████████ did not consider that ██████████ was violating the transit subsidy directive.³ ██████████ viewed the parking pass offer as a perk that ██████████ accommodated for ██████████ because of the long hours that ██████████ was putting into the job. ██████████ had a lot on his plate. He was providing assistance to the Deputy Staff Director and restructuring the Office of Human Resources. ██████████ offered ██████████ the parking benefits for ██████████'s convenience.

██████████ acknowledged that ██████████ was not in compliance with the FEC Directive. ██████████ had not thought about the Directive or this issue before ██████████ interview with the OIG. ██████████ advised ██████████ would pay back the transit benefits that ██████████ received during the months ██████████ drove to work.

On September 11, 2008, ██████████ advised that ██████████ provided the FEC Finance Office with a check in the amount of \$210 for metro fare benefits ██████████ received. The FEC Finance Office confirmed that this payment from ██████████ in the amount of \$210 was processed on September 16, 2008. ██████████ also agreed to turn in the temporary parking permit ██████████ used to the Office of Administrative Services.

B. Alleged Reprisal for Filing an OIG Complaint

Allegation 2: ██████████ retaliated against ██████████ for filing an OIG complaint.

On ██████████, 2008, ██████████ filed a complaint with the OIG, alleging that ██████████ retaliated against ██████████ because ██████████ had previously filed an OIG complaint against ██████████. Since ██████████ had made protected disclosures to the OIG, a reprisal investigation was initiated pursuant to section 7(c) of the Inspector General (IG) Act. Under the IG Act, federal employees in authority are prohibited from taking or threatening personnel action against an employee as a reprisal for making a complaint, or disclosing information to an Inspector General.⁴

³ As ██████████, ██████████ is responsible for overseeing the administration of the FEC transit benefit program.

⁴ 5 U.S.C. App. 3 § 7(c)

In August 25th reprisal complaint, [redacted] alleged three acts of retaliation: first, that [redacted]; secondly, [redacted]; and thirdly, that [redacted]. [redacted] claimed that [redacted] gave a [redacted] to the FEC on [redacted]. After this notice was given, [redacted] claimed [redacted] met with [redacted] upgrading [redacted] in order to [redacted] employment at the FEC. [redacted] said [redacted] learned on [redacted] 2008, from [redacted], that [redacted].

The findings in the OIG investigation did not substantiate [redacted]'s reprisal allegation. After conducting interviews with eight FEC employees, including two Commissioners⁶, the OIG found no evidence indicating that [redacted] knew [redacted] had made protected disclosures to the OIG on [redacted]. Furthermore, the evidence failed to support [redacted]'s claim that [redacted].⁷

[redacted] alleged two other acts of retaliation. First, [redacted] claimed that [redacted] also alleged that [redacted] claimed that [redacted].

⁵ In August 2008, the [redacted] consisted of Commissioner [redacted] and Commissioner [redacted].

⁶ During the reprisal investigation, the OIG interviewed the following FEC employees: Commissioner [redacted]; Commissioner [redacted]; [redacted]; former [redacted]; former [redacted]; [redacted]; and [redacted].

⁷ The OIG interviewed Commissioner [redacted], Commissioner [redacted], and [redacted]; and reviewed meeting notes prepared by Commissioner [redacted]'s Executive Assistant [redacted], concerning an August 22nd meeting between Commissioner [redacted] and [redacted]. These interviews and meeting notes did not corroborate [redacted]'s claim that the FEC Personnel Committee [redacted].

The OIG investigation found that [REDACTED]. However, investigative interviews revealed that [REDACTED].

There was no evidence found to suggest that [REDACTED] because of protected disclosures [REDACTED] made to the OIG.

With regards to the [REDACTED], the OIG concluded that [REDACTED] would not constitute a “personnel action” prohibited under the reprisal provision of the IG Act, nor the statutory definition under the Whistleblower Protection Act.⁹ Furthermore, the Office of General Counsel looked into the [REDACTED] issue after it was brought to the attention of Commissioners. When [REDACTED] was questioned by OGC, [REDACTED] denied [REDACTED]. For the reasons stated above, [REDACTED]’s reprisal allegation against [REDACTED] was unsubstantiated.

C. Alleged Improper Setting of Senior Level Pay

Allegation 3: [REDACTED] set [REDACTED] own salary when he was appointed to Acting [REDACTED] in violation of FEC Personnel Instruction 319.1.

On August 28, 2008, the OIG received a complaint alleging that [REDACTED] had set [REDACTED] own pay, without Commission approval, after the Commission voted to appoint [REDACTED] to the Acting [REDACTED] position. It was alleged that the paperwork on [REDACTED]’s appointment was circulated for a Commission vote, with the salary column left blank. It was further alleged that [REDACTED] increased his own salary by approximately seven steps, from a GS 15/3 salary of \$123,006, to approximately \$140,000 on the Senior Level (SL) pay scale.

The OIG initiated an investigation to determine if FEC pay setting policies were violated. The FEC pay setting policy applicable to promotions to an SL position, FEC Personnel Instruction 319.1, states:

A “current Federal employee appointed to an SL position is entitled to have his or her base pay set at the minimum of the SL rate which exceeds his or her existing rate of basic pay by not less than two step-increases of the grade from which he is promoted or transferred.

⁸ The OIG interviewed [REDACTED], Associate General Counsel [REDACTED], and [REDACTED], regarding the reason [REDACTED] was placed on administrative leave.

⁹ See 5 U.S.C. § 2302(a)(2)(A)

This initial rate may be set higher with advance Commission approval. The Commission may take into consideration the selectee's highest previous rate, relative level of responsibilities of the position being filled, comparable Federal Executive pay, the unusually high or unique qualifications and skills of the selectee, or a special need of the Commission for the selectee's services."¹⁰

The Commission Secretary furnished to the OIG a set of documents, known as a "voting package," which had been circulated to the Commission, in connection with the August 14, 2008, vote to temporarily appoint ██████████ as the Acting ██████████. A review of this voting package confirmed that ██████████'s new salary was omitted from the documents, specifically from the salary block on ██████████'s Notice of Personnel Action (SF 52). The SF 52 Notice, which showed a blank box for the salary, was signed by the former ██████████ Commissioner ██████████. A review of the voting package also showed that all six Commissioners voted to approve ██████████'s senior level appointment; and there were no Commission objections made as a result of the salary omission.

Commissioner ██████████, who was the FEC ██████████ the time, was interviewed regarding the allegation. In response to questions, ██████████ advised:

██████████ understood that ██████████ was to be bumped up in pay to approximately \$150,000. The Commission wanted to make ██████████'s salary comparable to what the previous ██████████ was earning. The ██████████ position has a lot more responsibilities, so it was expected that his ██████████'s] pay would increase. A raise of approximately \$25,000 does not seem unusual. The FEC Personnel Instruction established a "minimum" pay level, but it did not prohibit a higher salary. ██████████ did not recall the actual salary figure that was discussed for ██████████ around the time of the vote in August 2008. However, ██████████'s new salary of \$147,431 is consistent with ██████████'s understanding of what ██████████'s salary was going to be. At the time he signed ██████████'s SF 52, he [Chairman ██████████] was not concerned that the salary pay figures were left off of the form.

Based on former ██████████'s statement, and a full Commission vote with no objection to the salary omission, the investigation did not support a finding that ██████████ set ██████████ own salary without Commission approval. This allegation was, therefore, not substantiated.

¹⁰ FEC Personnel Instruction 319.1: Senior Level Pay, 8.B.1, pg.6, effective March 2, 2005.

IV. FINDINGS AND CONCLUSION

The transit benefit allegation was substantiated. The investigation found that [REDACTED] received FEC-paid parking and transit subsidy benefits, during the months of April thru July of 2008. The investigation found that during the months of May, June, and July of 2008, [REDACTED] collected full transit benefits, but did not commute on public transportation for more than 50% of the business days in these months. Based on these findings, the OIG found that [REDACTED] did not comply with requirements under Commission Directive 54.

The reprisal allegation was unsubstantiated. The investigation found no evidence to indicate that [REDACTED] knew or suspected that [REDACTED] filed an OIG complaint. The investigative findings also did not support [REDACTED]'s claim that [REDACTED] was denied a promotion, or even being considered for one.

The improper pay setting allegation was unsubstantiated. The investigation found that [REDACTED] had approval from the Chairman to set [REDACTED] salary amount, when [REDACTED] was appointed to the Acting [REDACTED] position. The investigation further revealed there were no objections from the Commission when [REDACTED]'s salary was omitted from the voting package for [REDACTED] appointment.

As a result of this investigation, [REDACTED] repaid transit subsidies totaling \$210 to the FEC. The OIG makes no recommendations regarding [REDACTED]'s conduct; however, it should be noted that [REDACTED] is no longer employed at the FEC. Other allegations made against [REDACTED] will be referred to the Acting Staff Director.

V. PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENT

**Summary of 26 allegations made against [REDACTED]
submitted to the OIG in eight (8) separate complaints
between July 23, 2008, and January 26, 2010**

Summary of 26 allegations made against [REDACTED], in eight (8) separate complaints to the OIG, submitted between July 23, 2008, and January 26, 2010				
	Date Received	Subject of Complaint	Allegation	Disposition
1	07/23/08	[REDACTED]	Alleged improper receipt of transit subsidy benefits/FEC parking benefits.	Investigated – Substantiated
2	08/11/08	[REDACTED]	Alleged improper hiring of the [REDACTED]: Position was allegedly not competed and it was upgraded without a desk audit.	Referred to Management
3	08/11/08	[REDACTED]	Alleged cronyism: improper hiring of [REDACTED].	Referred to Management
4	08/25/08	[REDACTED]	Alleged reprisal against [REDACTED] for filing an OIG complaint.	Investigated – Not Substantiated
5	08/28/08	[REDACTED]	Alleged improper pay setting of [REDACTED] salary, as the Acting [REDACTED], in violation of FEC Senior Level pay setting policy.	Investigated – Not Substantiated
6	06/04/09	[REDACTED]	Alleged improper upgrading of two positions in the Administrative Services Division, from a GS-7 to GS-8, and a GS-11 to GS-12.	Referred to Management
7	06/04/09	[REDACTED]	Alleged misuse of a contractor's ([REDACTED]) services to upgrade the Director of Human Resources position from a GS-15 to a Senior Level. Position description allegedly contained inaccuracies and was not reviewed or approved by the supervisor (Staff Director).	Referred to Management
8	07/14/09	[REDACTED]	The [REDACTED] allegedly kept three of his employees away from OPM Auditors.	Referred to Management
9	07/14/09	[REDACTED]	Alleged improper upgrading of the [REDACTED] position to facilitate a promotion for [REDACTED].	Referred to Management
10	07/14/09	[REDACTED]	Alleged improper hiring of [REDACTED] at a [REDACTED] level, when [REDACTED] allegedly had no prior [REDACTED] experience; it was [REDACTED] first federal government job; there was no position description; and [REDACTED] graded the position [REDACTED] despite a prior personal relationship with [REDACTED].	Referred to Management
11	07/14/09	[REDACTED]	Alleged improper upgrading of positions in the Finance Office despite a reduction in duties resulting from electronic systems/outsourced service providers.	Referred to Management
12	07/14/09	[REDACTED]	Alleged rumor that [REDACTED] said he has "the Chairman in his pocket" and he "runs to the Chairman for protection whenever questioned about anything."	Referred to Management
13	07/14/09	[REDACTED]	Alleged retaliation against [REDACTED].	Referred to Management

Summary of 26 allegations made against [REDACTED], in eight (8) separate complaints to the OIG, submitted between July 23, 2008, and January 26, 2010				
	Date Received	Subject of Complaint	Allegation	Disposition
14	07/14/09	[REDACTED]	Alleged improper selection of staff to be interviewed for the Office of Personnel Management (OPM) audit.	Referred to Management
15	07/14/09	[REDACTED]	Alleged improper grant of "same day security clearances" to several staff in the Commissioners' offices, in order to get computer access.	Referred to Management
16	11/10/09	[REDACTED]	Alleged personal relationship between [REDACTED] and [REDACTED].	Referred to Management
17	11/10/09	[REDACTED]	Alleged improper promotion of [REDACTED] without experience.	Referred to Management
18	11/10/09	[REDACTED]	Alleged improper supervision of staff and operations in the Administrative Services Division by the [REDACTED] without authority.	Referred to Management
19	11/10/09	[REDACTED]	Alleged misuse of government funds to pay for refreshments for FEC staff during a team building exercise. The Office of Chief Financial Officer (OCFO) allegedly approved the improper payment for refreshments.	Referred to Management
20	11/10/09	[REDACTED]	[REDACTED] allegedly made [REDACTED] work from home for three weeks to create documentation for the OPM audit. The documentation was then allegedly backdated for the OPM audit.	Referred to Management
21	11/10/09	[REDACTED]	[REDACTED] was allegedly escorted from his last position at the [REDACTED] for gross misconduct.	Referred to Management
22	01/26/10	[REDACTED]	Alleged compensatory time abuse.	Referred to Management
23	01/26/10	[REDACTED]	Alleged improper downgrading of the [REDACTED] position to facilitate [REDACTED]'s retirement.	Referred to Management
24	01/26/10	[REDACTED]	Alleged improper upgrading of [REDACTED] positions, in July 2009, from a GS-13 to a GS-14.	Referred to Management
25	01/26/10	[REDACTED]	Alleged improper influence of contractor [REDACTED], to assess a position description for [REDACTED] as a GS-15, rather than a GS-14.	Referred to Management
26	01/26/10	[REDACTED]	Alleged improper hiring of additional staff in the [REDACTED] and the [REDACTED] without FTE capacity.	Referred to Management



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CASE CLOSING MEMORANDUM

Case #: INV-09-01	Prepared By: J. C. THURBER
Case Title: ██████████	
Date of Report: April 7, 2011	
Subject: Transit Subsidy Abuse	

Hotline Complaint HL-08-05 was opened on August 8, 2008, when ██████████ ██████████ made a referral to the OIG ██████████ the FEC transit benefit subsidy program. ██████████ alleged that records showed ██████████ was receiving both parking benefits and transit subsidy benefits. Parking and transit subsidy records were reviewed and confirmed ██████████'s participation in both benefits in violation of Commission Directive 54. During the review of the hotline complaint, SmarTrip records were obtained from the Washington Metropolitan Transit Authority (WMATA). Kastle systems records showing building access entries made by ██████████ were also obtained from ██████████. A review of these records indicated that ██████████ may have received both parking and transit subsidy benefits during the period from May 2008 through September 2008. Based on this information, an investigation was opened on December 31, 2008.

OIG Disposition:

The OIG issued a Report of Investigation to the Commission and FEC management on May 11, 2010. In the report, the OIG recommended: that management consider recovering transit subsidy overpayments in the amount of \$805.60 from ██████████, and any other monies owed since the period of the OIG's investigation; that management consider whether any other action is necessary in regards to ██████████ based on this investigation, if any; and that the Office of Human Resources assess ██████████'s eligibility to continue her participation in the transit benefit program.

On February 17, 2011, FEC management advised the OIG that the following action had been taken:

1. ██████████ was issued an oral admonishment which was confirmed in writing.
2. ██████████ will be required to repay the \$805.60 in transit benefit received during her period of ineligibility as determined by the OIG investigation.

3. [REDACTED] has the option of withdrawing from the program or submitting to monitoring of [REDACTED] use of the program in FY 2011. If [REDACTED] chooses to submit to monitoring, [REDACTED] will be required to comply strictly with Directive 54, to avoid placing personal funds on the SmartTrip card [REDACTED] uses for commuting, and to obtain from WMATA quarterly a report of [REDACTED] use of the card for the preceding three months. These reports will be reviewed by [REDACTED] supervisor. If [REDACTED] misses any deadline to submit a report, uses Metro so infrequently that [REDACTED] falls out of eligibility for the program, or otherwise does not comply with Directive 54, [REDACTED] will be removed from the program.

No further investigative activity is required. Therefore, this investigation is closed.

Concurrence: _____
Lynne McFarland, Inspector General Date

**FEDERAL ELECTION COMMISSION
OFFICE OF INSPECTOR GENERAL**



Report of Investigation

■■■■■■■■■■ ■■■■■■■■■■'s *Transit Benefit Participation*

Case Number INV-09-01

May 11, 2010

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

<u>Table of Contents</u>		<u>Page</u>
I.	Executive Summary	1
II.	Allegation	2
	██████████ allegedly carpooled to work with her ██████████, while collecting transit subsidies, in violation of FEC Commission Directive 54.	
III.	Background	2
	A. FEC Transit Benefit Program: Directive No. 54	2
	B. Scope of the Investigation	3
IV.	Investigation Details	3
	A. Transit Benefit Program Application and Re-Certifications	3
	B. FEC Garage Access and Parking Activity	5
	C. Commute via Public Transportation	5
	D. Interview of ██████████ ██████████	7
	E. Interview of ██████████ ██████████	8
V.	Findings	10
VI.	Recommendations	10
VII.	Privacy Act and Freedom of Information Act Notice	11
	Attachment List	12

I. Executive Summary

In August 2008, the Office of Inspector General (OIG) conducted an audit follow-up on the FEC transit benefit program, which revealed that ██████████ (C ██████████ ██████████ ██████████), may have received a Federal parking benefit, while simultaneously collecting transit subsidies, in violation of FEC Commission Directive No. 54. The allegation arose after LAZ Parking, the FEC's parking management company, provided records showing that from January 2008, through July 2008, ██████████ purchased a monthly parking permit, to park ██████████ vehicle in the FEC garage.

FEC Commission Directive No. 54, "Employee Transit Benefit Program," requires that an employee use public transportation "a minimum of 50% of the available number of commuting days (business days) per month..." If an employee regularly commutes to the FEC office using public transportation, but for whatever reason, does not commute on public transportation for at least 50% of the business days in a given month, then they are only entitled to receive one-half (50%) of their full transit benefit for that month, rounded up to the next five dollar increment.

The OIG found that during the 23 month period investigated, September 2007 to July 2009, ██████████ ██████████ did not comply with FEC Directive 54, *Employee Transit Benefit Program*, because she withdrew transit benefits in excess of amounts she was entitled to claim under the policy. The investigation found that ██████████ received \$805.60 in transit subsidies, for which she was not entitled to receive. In 15 out of the 23 months investigated, ██████████ did not commute by public transportation on at least 50% of the monthly business commute days.

The investigation determined that ██████████ ██████████ carpooled to work with ██████████, or drove ██████████ car to work, and received Federal parking benefits, in total, more often than ██████████ commuted to work on public transportation. Over the 23 month period, ██████████ claimed and received \$2,605.60 in transit benefits; yet ██████████ actual commuting costs for the period were only \$1,380.80; and under the 50% rule in Directive 54, ██████████ was only entitled to receive \$1,800.00. The investigation found that ██████████ used \$926 of the excess transit subsidies ██████████ received to pay for parking at the Largo Metro station.

Based on these findings and a review of Commission Directive 54, the OIG recommends that management consider recovering transit subsidy overpayments in the amount of \$805.60 from ██████████ and any other monies owed since the period of the OIG's investigation. The OIG also recommends that management consider whether any other action is necessary in regards to ██████████ based on this investigation, if any. We also recommend that the Office of Human Resources assess ██████████ ██████████'s eligibility to continue ██████████ participation in the transit benefit program, based on ██████████ actual commute pattern, including carpool participation and receipt of Federal parking benefits.

II. Allegation

[REDACTED] (C [REDACTED], carpooled to work with [REDACTED], while collecting transit subsidies, in violation of FEC Commission Directive 54.

III. Background

A. FEC Transit Benefit Program: Directive No. 54

The FEC transit benefit program encourages employees to commute to and from work, by means other than single-occupant vehicles. The purpose of the FEC transit subsidy program is to provide financial incentives to employees who “regularly commute” via public transportation. For the purposes of this program, “regularly commute” means that “*the employee commutes via public transportation on a regular and recurring basis.*”

To be eligible for transit benefits, FEC Commission Directive No. 54, “Employee Transit Benefit Program,” requires that an employee use public transportation “*a minimum of 50% of the available number of commuting days (business days) per month...*” If an employee regularly commutes to the FEC office using public transportation, but for whatever reason, does not commute on public transportation for at least 50% of the business days in a given month,¹ then they are only entitled to receive one-half (50%) of their full transit benefit for that month, rounded up to the next five dollar increment.²

Commission Directive 54 places responsibility on the transit benefit recipient to elect the correct subsidy amount each month (either the full amount or 50% of the transit benefit). The amount elected each month should be based on the employee’s anticipated use of public transportation during the next month; or based on the employee’s actual use of public transportation during the previous month. Employees are required to notify the Personnel Office, or submit a new transit application, when their commuting pattern or cost changes; or if they become ineligible to continue participation in the program.

Commission Directive No. 54 prohibits employees who commute in a private carpool, or who receive a “Federal parking benefit,” from participating in the transit benefit program.

¹ There are approximately 20 business days each month, so approximately 10 business days would represent 50% of the total business days each month.

² If an FEC employee receives transit subsidy benefits of \$115 each month, but for whatever reason, will **not** commute to work 50% or more of the business days in a particular month; then the employee is only entitled to receive \$60 in subsidy benefits ($\$115 \times .5 = \57.50 , rounded up to \$60).

According to the Directive, a “Federal parking benefit” provides an employee with vehicle parking at a cost lower than local prevailing commercial parking rates.

B. Scope of the Investigation

During the investigation, the OIG gathered and reviewed agency records pertaining to [REDACTED] [REDACTED]. These records included [REDACTED]’s initial transit benefit application, plus annual certifications she filed for years 2007, 2008 and 2009. The OIG also reviewed temporary FEC-paid parking permit sign out logs; Kastle Systems keycard access data; and time and attendance records (i.e. leave usage data) from September 2007, through July 2009.

In addition, the OIG reviewed records obtained from outside entities. These records included transit activity reports for [REDACTED]’s SmarTrip card account (# [REDACTED]), which were obtained from the Washington Metropolitan Area Transit Authority (WMATA). These WMATA reports showed monthly transit subsidy disbursements and Metro commute activity for the period September 4, 2007, through July 31, 2009. The OIG also reviewed employee paid parking records obtained from LAZ Parking, LTD.

During the investigation, the OIG interviewed [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED], a former [REDACTED], in the [REDACTED] [REDACTED] [REDACTED]). Since [REDACTED] [REDACTED] is in a bargaining unit position, [REDACTED] had union representation during the OIG interview.

IV. Investigation Details

In August 2008, an OIG audit follow-up of the FEC transit benefit program revealed that [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED], may have collected transit subsidies, while [REDACTED] received a Federal parking benefit, in violation of FEC Commission Directive No. 54. Under Directive 54, FEC employees who carpool to work, or receive a Federal parking benefit, are not eligible to participate in the transit benefit program. (Attachment 1)

The FEC’s parking management company, LAZ Parking, provided records during the OIG’s 2008 audit follow-up, which listed all FEC employees who purchased monthly parking permits to park their vehicles in the FEC garage. These records showed that from January 2008, through July 2008, [REDACTED] purchased a monthly parking permit for [REDACTED] vehicle ([REDACTED]). (Attachment 2)

A. Transit Benefit Program Application and Re-Certifications

As part of the OIG’s 2008 audit follow-up testing activity, the names of FEC employee parking permit holders were checked against the names of FEC transit subsidy recipients. This

comparison revealed that on August 7, 2007, [REDACTED] signed and submitted an initial *FEC Transit Subsidy Program Application* to the Office of Human Resources to participate in the transit benefit program. Since that time, [REDACTED] submitted three subsequent applications to recertify [REDACTED] eligibility for participation in the program. (Attachment 3)

Table 1. [REDACTED] Transit Benefit Application and Re-Certifications

Date	Form Type	Employee Calculated Commute Cost Per Month	Maximum Allowable Monthly Claim under the Program
August 7, 2007	Initial application	\$118	\$110
December 11, 2007	Re-certification	\$118	\$115
February 12, 2009	Re-certification	\$142	\$120
July 9, 2009	Change	\$142	\$142

A review of these applications showed that [REDACTED] calculated [REDACTED] monthly commute costs based on 20 commute days each month, by Metro subway, from the [REDACTED] Metro station to the Metro Center subway station in Washington, DC. On these transit applications, [REDACTED] made certifications to comply with the program, including the following:

- *I certify I am eligible for a public transportation fare benefit. I will use it for my daily commute to and from work. I will not give, sell, or transfer it to anyone else.*
- *I certify I am not a member of a carpool. Furthermore, I do not receive disability or executive parking privileges.*
- *I certify that the monthly transit benefit I receive does not exceed my monthly commuting costs.*
- *I certify my usual monthly public transportation commuting costs (excluding any parking costs) is the amount listed above (amount is supported by completed worksheet).*

[REDACTED], former [REDACTED], [REDACTED], was interviewed by the OIG. [REDACTED] was questioned about an email she sent to [REDACTED] on September 23, 2008, in which [REDACTED] questioned [REDACTED] about receiving transit benefits, while parking in the FEC garage. (Attachment 4) During this interview, [REDACTED] advised:

[REDACTED] phoned [REDACTED] in response to the email [REDACTED] sent on September 23, 2008. During their telephone conversation, [REDACTED] questioned [REDACTED] about the receipt of both benefits. In response to the questions, [REDACTED] said that the parking pass belonged to [REDACTED] who is [REDACTED]. [REDACTED] said that [REDACTED] rides the Metro to work every day.

explained to that () does not ride into work with () advised that and have different schedules because has to .³

B. FEC Garage Access and Parking Activity

During the investigation, the Administrative Services Division provided Kastle Systems building access reports on keycards assigned to () and (), () () who is also employed at the FEC.⁴ Since Kastle keycard reports are stored for only 90 days, the OIG could only obtain reports covering the periods of May 2008, through August 2008; October 2008, through December 2008; May 2009, through July 2009; and November 2009, through February 2010. (Attachment 5)

A review of the Kastle Systems data indicated that () carpooled to work with () on numerous occasions; and on some occasions, both () and () drove to the FEC and parked separate cars in the garage. The Kastle Systems data showed that () often used () keycard to access the building garage entrance from the street (code ()), as detailed in (Attachment 5); or to access the entrance to the building from the garage (code ()), sometimes within minutes of garage access by (). (Attachment 5)

The OIG obtained FEC-paid parking permit records from the Administrative Services Division. These agency records identified FEC employees who requested and were issued temporary parking permits. A review of these records showed that () requested and was issued a second parking permit for the FEC garage, on a temporary basis, for the following dates: 03/10/08 – 03/13/08; 04/01/08 – 04/04/08; 06/20/08 – 06/26/08; 10/08/08; 02/26/09; 05/07/09 – 05/11/09; 05/20/09 – 05/26/09; and 01/12/10 – 01/15/10. (Attachment 6)

C. Commute via Public Transportation

During the investigation, the OIG obtained WMATA records on ()'s SmarTrip transit card activity during the period September 2007, through July 2009. A review of these activity reports indicated that in 15 out of 23 months, () failed to commute to the FEC a minimum of 50 percent of the commutable days per month (Attachment 7). This transit data is summarized in Table 2 on the following page.

³ () was interviewed by the OIG on November 12, 2008.

⁴ () was assigned Kastle Systems keycard #291-01867; () was assigned keycard ().

Table 2. Summary of [REDACTED]'s Transit Activity

[REDACTED] Transit Activity Summary											
	Month	Transit Benefit Claimed	Total Possible Commute Days in Month	Actual Full Days Commuted	Full Day Monthly Commute Costs	Actual Partial Days Commuted	Actual Partial Days Monthly Commute Costs	Total Actual Commute Costs per Month	Monthly Parking Payments Made	Commuted on WMATA 50% or More?	50% Rule Claims Allowed
1	Sep-07	\$110.00	19	9	\$53.10	1	\$2.95	\$56.05	\$35.00	Y	\$110.00
2	Oct-07	\$110.00	22	8	\$47.20	1	\$2.95	\$50.15	\$31.50	N	\$55.00
3	Nov-07	\$110.00	20	12	\$70.80	3	\$8.85	\$79.65	\$52.50	Y	\$110.00
4	Dec-07	\$110.00	20	10	\$59.00	1	\$2.95	\$61.95	\$38.50	Y	\$110.00
5	Jan-08	\$110.00	21	6	\$42.60	1	\$3.55	\$46.15	\$29.75	N	\$55.00
6	Feb-08	\$115.00	20	5	\$35.50	2	\$7.10	\$42.60	\$29.75	N	\$60.00
7	Mar-08	\$115.00	21	6	\$42.60	2	\$7.10	\$49.70	\$34.00	N	\$60.00
8	Apr-08	\$115.00	22	11	\$78.10	2	\$7.10	\$85.20	\$55.25	Y	\$115.00
9	May-08	\$115.00	21	7	\$49.70	1	\$3.55	\$53.25	\$34.00	N	\$60.00
10	Jun-08	\$115.00	21	1	\$7.10	5	\$17.75	\$24.85	\$21.25	N	\$60.00
11	Jul-08	\$115.00	22	10	\$71.00	5	\$17.75	\$88.75	\$59.50	Y	\$115.00
12	Aug-08	\$115.00	21	6	\$42.60	3	\$10.65	\$53.25	\$38.25	N	\$60.00
13	Sep-08	\$115.00	21	12	\$85.20	2	\$7.10	\$92.30	\$59.50	Y	\$115.00
14	Oct-08	\$115.00	22	9	\$63.90	3	\$10.65	\$74.55	\$51.00	N	\$60.00
15	Nov-08	\$115.00	18	5	\$35.50	2	\$7.10	\$42.60	\$29.75	N	\$60.00
16	Dec-08	\$115.00	21	5	\$34.30	2	\$7.10	\$41.40	\$25.50	N	\$60.00
17	Jan-09	\$115.00	20	7	\$49.70	1	\$3.55	\$53.25	\$34.00	N	\$60.00
18	Feb-09	\$115.00	19	8	\$56.80	3	\$10.65	\$67.45	\$46.75	Y	\$115.00
19	Mar-09	\$115.45	22	7	\$49.10	3	\$10.65	\$59.75	\$41.75	N	\$60.00
20	Apr-09	\$94.80	22	5	\$35.50	5	\$17.75	\$53.25	\$38.25	N	\$60.00
21	May-09	\$120.00	20	10	\$71.00	3	\$10.65	\$81.65	\$55.25	Y	\$120.00
22	Jun-09	\$120.00	22	7	\$49.70	3	\$10.65	\$60.35	\$42.50	N	\$60.00
23	Jul-09	\$110.35	22	8	\$55.60	2	\$7.10	\$62.70	\$42.50	N	\$60.00
	Totals	\$2,605.60	479	174	\$1,185.60	56	\$195.20	\$1,380.80	\$926.00	8 of 23 > or = 50% 15 of 23 < 50%	\$1,800.00

Did not commute 50% of the monthly business days by public transportation.
Amount of Overpayment: \$805.60 (\$2,605.60 - \$1,800 = \$805.60).

Two way commute > or = to 50% of monthly commutable days.
Adding partial commute days is > or = to 50% of monthly commutable days.

Despite the fact that [REDACTED] commuted to work by car more often than not, each month [REDACTED] claimed full subsidy amounts, instead of claiming just the 50% [REDACTED] was entitled to, for 15 months, under Directive 54.⁵ During the 23 month period, September 2007, to July 2009, [REDACTED] claimed transit subsidies of \$2,605.60. During this same period, [REDACTED] only incurred Metro transit commuting costs of \$1,380.80; [REDACTED] received excess transit subsidies of \$1,224 over [REDACTED] actual public transportation costs. According to the WMATA records, [REDACTED] used \$926 of the excess transit subsidies to pay for parking, at the [REDACTED] Metro station.

Under Commission Directive 54, [REDACTED] was only authorized to receive 50% of [REDACTED] regular monthly commuting costs, during the 15 months when [REDACTED] commuted by public transportation for less than 50% of the monthly business commute days. Since [REDACTED] claimed [REDACTED] full subsidy amounts during these 15 months, [REDACTED] received transit subsidies of \$805.60, for which [REDACTED] was not entitled to.

D. Interview of [REDACTED]

On March 12, 2010, the OIG interviewed [REDACTED] regarding [REDACTED] transit subsidy claims. [REDACTED] had union representation during the interview. [REDACTED] was asked to explain why in 15 out of 23 months, [REDACTED] did not commute 50 percent of the time by public transportation. In response to questions, [REDACTED] advised:

- *On some days, [REDACTED] commutes to work with [REDACTED] (rides to work with [REDACTED] and/or rides home in [REDACTED] car). Before participating in the transit subsidy program, [REDACTED] regularly carpooled to work with [REDACTED] husband.*
- *[REDACTED] began using transit subsidy benefits in August or September 2007, so [REDACTED] could have time after [REDACTED], and [REDACTED].*
- *[REDACTED] drops off [REDACTED] at [REDACTED] in the morning and [REDACTED] picks up [REDACTED] around 4:30 pm at the earliest. [REDACTED] takes the Metro from the FEC to [REDACTED], gets the car and drives to [REDACTED] to pick [REDACTED] up.*
- *When there is an activity at [REDACTED], [REDACTED] rides to work by car with [REDACTED]. If [REDACTED] has a [REDACTED], [REDACTED] drives to the Metro station to drop off [REDACTED] car; then [REDACTED] picks [REDACTED] from Metro and [REDACTED] attend [REDACTED]. On these occasions, [REDACTED] commutes with [REDACTED] to the FEC together in the car. [REDACTED] would leave [REDACTED] car at the Metro station so [REDACTED] can pick up [REDACTED] in the evening; since [REDACTED] does not get off work until [REDACTED]. If [REDACTED] do not pick up [REDACTED].*
- *[REDACTED] sometimes drives [REDACTED] car to work. If [REDACTED] drives to work, [REDACTED] will get [REDACTED] a temporary FEC-paid parking pass for the garage. [REDACTED] does not request [REDACTED] own temporary parking pass, because [REDACTED] thought it was a management benefit. [REDACTED] sometimes*

⁵ See Commission Directive 54, Section V.2 Alternate Fare Media Calculation, pg 3.

has a need for temporary parking when [REDACTED] travels, because [REDACTED] has to [REDACTED]
[REDACTED]

- On some occasions, [REDACTED] and [REDACTED] will [REDACTED] drive separate cars to work, when one of [REDACTED] needs to go to the repair shop. [REDACTED] so one of them is not stuck in [REDACTED], where [REDACTED] get [REDACTED].
- On some occasions, [REDACTED] will work late and gets a ride home with [REDACTED].
- [REDACTED] sometimes will take [REDACTED] car parked in the FEC garage to go pick up [REDACTED] and then return the car to the FEC. On these occasions, [REDACTED] [REDACTED] in the car. Sometimes [REDACTED] may pick up [REDACTED] and return to the FEC; and again, they [REDACTED].
- [REDACTED] recalled an email sent to her in 2008 from [REDACTED], regarding [REDACTED] name still being on the list for parking in the FEC garage. At that time, [REDACTED] told [REDACTED] that it was [REDACTED] parking spot, and that [REDACTED] takes the Metro to work. It never came up during conversation with [REDACTED] as to whether [REDACTED] sometimes still rides to work with [REDACTED]. On a "perfect day," [REDACTED] does take the Metro to work.
- Since August or September 2007 [REDACTED] has used [REDACTED] SmarTrip card to pay for parking. [REDACTED] probably has not put any of [REDACTED] own money on the SmarTrip card during the past year. After [REDACTED] was interviewed by the OIG, [REDACTED] purchased a second SmarTrip card and placed \$50.00 on it.
- [REDACTED] only recently became familiar with the FEC transit policy. [REDACTED] did not read the transit application very carefully when [REDACTED] completed and signed the forms. [REDACTED] could not say whether [REDACTED] had or had not read the rules completely when [REDACTED] applied for the transit benefits program.
- [REDACTED] did not think [REDACTED] was doing anything wrong, by riding with [REDACTED] to or from the FEC, and collecting transit benefits. [REDACTED] thought [REDACTED] commuted 50% or more per month using the Metro. [REDACTED] saw the 50% requirement as having taken two weeks off of work in a month. [REDACTED] has never taken that much time off. [REDACTED] was surprised to learn [REDACTED] did not commute 50% or more in the months in question. [REDACTED] would have sworn [REDACTED] commuted using Metro more than that.

E. Interview of [REDACTED] [REDACTED]

[REDACTED] [REDACTED] was interviewed by the OIG on February 25, 2010. [REDACTED] statements during the interview were consistent with those made by [REDACTED] [REDACTED] [REDACTED] [REDACTED] advised:

- [REDACTED] drives to and from the FEC and parks his [REDACTED] in the basement [REDACTED].
- [REDACTED] current parking permit fee is \$227 per month. This fee is paid to the attendant from a [REDACTED] [REDACTED] pays the attendant each month. [REDACTED] has [REDACTED]

a second [REDACTED] [REDACTED] [REDACTED] [REDACTED] There may have been a few occasions since [REDACTED] became a transit benefit recipient where [REDACTED] paid the attendant [REDACTED].

- [REDACTED] standard work hours are [REDACTED], but if [REDACTED] is working on a project, [REDACTED] will call [REDACTED] and keep [REDACTED] posted on [REDACTED] planned departure time as it progresses. If [REDACTED] departure time gets too late, [REDACTED].
- If [REDACTED] cannot leave by 5:30 pm, [REDACTED] can take leave and go pick up [REDACTED] then return to the FEC to pick up [REDACTED]. If [REDACTED] does not take the Metro [REDACTED] (because [REDACTED] rides with [REDACTED] or is picked up later), then [REDACTED] drops [REDACTED] off at the Metro station so [REDACTED] can pick up [REDACTED] car. [REDACTED] never leave [REDACTED] car in the Metro overnight. [REDACTED] has safety concerns about [REDACTED] taking the Metro home late at night.
- Sometimes, if [REDACTED] is not feeling well, [REDACTED] will call in late to work, and then if feeling better, [REDACTED] will ride into the FEC with [REDACTED]. If [REDACTED] rides to work with [REDACTED] in the morning, then [REDACTED] rides home with [REDACTED] too, because there is no car for [REDACTED] at the Metro station.
- When the FEC is holding a conference in DC, [REDACTED]. In these instances, [REDACTED] alters [REDACTED] work schedule to [REDACTED]. [REDACTED] needs to drive the car to the FEC, so [REDACTED] gets [REDACTED] a temporary parking pass from the Administrative Services Division. [REDACTED] drives in on these occasions to reduce [REDACTED] commute time, and reduce how late s [REDACTED] will be from [REDACTED].
- For [REDACTED] requests a temporary parking pass from Administrative Services to drive to the FEC and park [REDACTED] car; then [REDACTED] and then drives [REDACTED] car to the FEC [REDACTED]. In the evening, [REDACTED] [REDACTED] each day to work when [REDACTED] is out of town, so [REDACTED] has better [REDACTED].
- [REDACTED] makes the requests for the temporary FEC-paid parking pass for [REDACTED] because [REDACTED] thought only managers could request an FEC-paid parking pass. Also, it is because of job responsibility ([REDACTED]) that creates the need for [REDACTED] to have to drive [REDACTED] to work.
- When [REDACTED] signs out a temporary FEC-paid parking pass, so [REDACTED] can have [REDACTED]. [REDACTED] is getting the parking passes for [REDACTED] for [REDACTED] cars. [REDACTED] saw a manager request and receive a parking pass years ago. [REDACTED] thought it would be better than if [REDACTED] had to pay for parking downtown. Management could always say no and not give [REDACTED] the pass. When [REDACTED] signed out the temporary parking permits for [REDACTED], [REDACTED] explained to Administrative Services the reason [REDACTED] needed the pass was to [REDACTED].

- *There are no written procedures for requesting an emergency or temporary pass. [REDACTED] assumed it was something managers could do, but general staff could not.*
- *[REDACTED] was under the impression that the transit benefits provided by the agency were not enough to cover all of [REDACTED] commute costs; so [REDACTED] thought [REDACTED] was adding [REDACTED] the card each month.*
- *[REDACTED] did not know that carpooling prevented transit subsidy program participation. [REDACTED] considers that when [REDACTED] rides into work with [REDACTED], [REDACTED] is still incurring a commute cost ([REDACTED]). [REDACTED] pays the cost for the commute.*

V. Findings

The OIG found that during the 23 month period investigated, September 2007 to July 2009, [REDACTED] [REDACTED] did not comply with FEC Directive 54, *Employee Transit Benefit Program*, and drew transit benefits in excess of amounts she was entitled to claim under the policy. The investigation found that:

- [REDACTED] received \$805.60 in transit subsidies, which [REDACTED] was not entitled to receive, under Commission Directive 54.
- In 15 out of the 23 months investigated, [REDACTED] did not commute on public transportation for 50% of the monthly business commute days.
- [REDACTED] carpoled to work with [REDACTED], or drove [REDACTED] car to work, and received Federal parking benefits, in total, more often than [REDACTED] commuted to work on public transportation.
- [REDACTED] claimed \$2,605.60 in transit benefits, during a 23 month period, when [REDACTED] actual commuting costs during this period was only \$1,380.80.
- [REDACTED] used \$926 of the excess transit subsidies [REDACTED] received to pay for parking at the [REDACTED] Metro station.

VI. Recommendations

Based on these findings and a review of Commission Directive 54, the OIG recommends that management consider the following:

- A recovery of transit subsidy overpayments that were made to [REDACTED] [REDACTED] which totaled \$805.60 for the period of investigation. Management should also determine whether additional funds are owed by [REDACTED] to the FEC for the period since July 2009.

- Management should consider whether any other action is necessary in regards to [REDACTED] based on this investigation, if any.
- An evaluation as to [REDACTED] [REDACTED]'s eligibility to continue [REDACTED] participation in the transit benefit program, based on [REDACTED] "regular and recurring" commute pattern, including [REDACTED] carpool participation and receipt of Federal parking benefits.
- FEC management should provide a response to the Inspector General within 60 days of this report documenting their action(s) taken or status of the recommendations contained in this report.

VII. Privacy Act and Freedom of Information Act Notice

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENTS

Attachments #	Description
1	FEC Commission Directive No. 54, effective August 15, 2001.
2	LAZ Parking, LTD Records on FEC employees receiving employee-paid monthly parking permits, for the months January 2008 – July 2008.
3	FEC Transit Subsidy Program Applications submitted by [REDACTED] [REDACTED]
4	Email from [REDACTED] to [REDACTED] [REDACTED] dated 09/23/08.
5	Kastle Systems History Reports for keycards assigned to [REDACTED] [REDACTED] and [REDACTED] [REDACTED]
6	FEC Temporary Parking Permit Sign-out Sheets obtained from the Administrative Services Division.
7	WMATA SmarTrip Transaction History Reports for SmarTrip card [REDACTED].



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CLOSING MEMORANDUM

Case #: INV-09-02	Prepared By: Joseph Duncan
Case Title: Clifton Gunderson	
Date of Report: 04/21/10	
Subject: CG Laptop Incident	

On February 10, 2009, Kent Nilsson, the Inspector General (IG) for the Federal Communications Commission (FCC) reported that his office received a laptop computer from Clifton Gunderson, which contained data of the Federal Election Commission (FEC). The OIG initiated an investigation into the alleged release of FEC data.

The investigation was conducted from February 10, through May 15, of 2009. It was determined that CG improperly released sensitive FEC data to the FCC without authorization. This unauthorized release was found to be accidental and limited only to the FCC OIG. No personally identifiable information was released. The investigation further determined that CG failed to comply with the FEC's data security requirements, including: Directive 58, *Electronic Records, Software and Computer Usage*; Mobile Computing Security Policy (58-4.3); and FEC Non-Disclosure Agreements. CG also failed to install, within a timely manner, encryption software on the laptop in question.

OIG Disposition: On June 3, 2009, the OIG issued a Report of Investigation to the Commission and FEC management, which included suggestions to improve the protection of sensitive FEC data. As a result of the OIG investigation, the FEC recovered \$5,984.90 in a settlement, which was offset from the final invoice owed to CG. Based on this result, this investigation will be closed.

Concurrence: _____
Jon Hatfield, Deputy Inspector General Date



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Lynne A. McFarland
Inspector General *LGM*

SUBJECT: Report of Investigation: The Clifton Gunderson Laptop Incident

DATE: June 4, 2009

This memorandum transmits the Office of Inspector General's (OIG) Report of Investigation: "*The Clifton Gunderson Laptop Incident*," dated June 3, 2009. Also included in this package for ease of reference is the internal report prepared by Clifton Gunderson LLP (CG), entitled "*Report on FEC Data Concern*," which is dated June 2, 2009. The CG report is also included in the OIG Report of Investigation as attachment 9.

On February 10, 2009, Kent Nilsson, the Inspector General (IG) for the Federal Communications Commission (FCC), contacted me and advised that his office received a laptop computer from CG, which contained data of the Federal Election Commission (FEC). CG has performed contract audits for both the FCC Office of Inspector General (OIG) and the FEC OIG. CG audited the FEC's annual financial statements, on behalf of the OIG, during the fiscal years (FY) 2004 through 2008. For these audit services, the FEC paid contract costs to CG totaling \$492,314.79.

Based on the information received from the FCC OIG, my office immediately initiated an investigation into the alleged release of FEC data. As a result of this investigation, my office determined that CG improperly released sensitive FEC data to the FCC without authorization. The FEC defines "sensitive information" in Commission Directive 58, as "*any data/information (whether in an electronic or non-electronic format), where loss, misuse, or unauthorized access to or modification of, could seriously hamper the Commission's ability to carry out its mandated functions.*" This unauthorized release was found to be accidental and limited only to the FCC OIG. No personally identifiable information was released.

During the investigation, my office further determined that CG failed to comply with the FEC's data security requirements, including: Directive 58, *Electronic Records, Software and Computer Usage*; Mobile Computing Security Policy (58-4.3); and FEC Non-Disclosure Agreements. For instance, CG failed to report the accidental disclosure to the FEC OIG. CG also failed to remove FEC data from its laptop at the conclusion of the FY 2007 audit, and prior to the laptop's transfer to the FCC. The OIG also found that CG failed to install, within a timely manner, encryption software on the laptop in question.

My office conducted this investigation from February 10, through May 15, of 2009. Investigative activities conducted during this period included seventeen (17) witness interviews; three meetings with CG partners; three meetings at the FCC to examine the laptop's hard drive; a review of the 402 FEC data files; and a review of FEC OIG records pertaining to the CG contract and audit services. CG cooperated with the OIG during the investigation.

Throughout this investigation, my staff and I met with, and communicated frequently with, Alec Palmer, the Chief Information Officer (CIO), and Edward Bouling, the Information Systems Security Officer (ISSO). My office provided the CIO and ISSO with regular updates on investigative activities. The CIO and ISSO provided my staff with technical subject matter assistance concerning data security requirements. It should also be noted that my staff received technical assistance during the investigation from IT and computer forensic personnel at the FCC OIG.

As a result of this incident, my staff offers three suggestions to the FEC to improve the protection of sensitive FEC data. These include: 1) incorporate contractor data security standards in all FEC contracts; 2) require post-contract certifications that FEC data has been removed from all laptops; and 3) improve the identification of FEC data that is, or should be, classified as "sensitive."

Recently, my staff met with the ISSO to discuss new data security standards for FEC contracts. As a result, the CIO and ISSO have implemented new "Minimum Contractor System Security Standards," which have already been incorporated into the OIG's new financial statement audit contract that was signed in April 2009. In addition, the OIG has implemented a new policy entitled "FEC OIG Contractor Security Standards," which will strengthen data security controls on all future OIG audit contracts.

The OIG would like to meet with the Commission to discuss the findings of this investigation. In the meantime, if you have any questions regarding the investigative report, please do not hesitate to contact me at 202-694-1015. The OIG appreciates the cooperation of the Commission and staff during the course of this investigation. Thank you.

cc: Tommie P. Duncan, General Counsel
Robert A. Hickey, Staff Director
Mary Sprague, Chief Financial Officer
Alec Palmer, Chief Information Officer
Lawrence Calvert, Co-Chief Privacy Officer
Edward F. Bouling, Information Systems Security Officer

FEDERAL ELECTION COMMISSION
OFFICE OF INSPECTOR GENERAL



Report of Investigation

The Clifton Gunderson Laptop Incident

Case Number INV-09-02

June 3, 2009

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

<u>Table of Contents</u>		<u>Page</u>
I.	Executive Summary	1
II.	Allegation	6
III.	Background	6
	A. FEC Contract No. FE4AC0065: Financial Statement Audit	7
	B. CG Staff Assigned to the FEC Contract	7
	C. CG’s End User Support and Administrative Staff	8
	D. FEC Directive 58 & Computer Security Training	9
	E. FEC Non-Disclosure Agreements	9
	F. CG Assurances to Secure Sensitive FEC Data	10
IV.	Investigation Details	11
	A. What FEC data was found on the CG laptop?	11
	B. How did FEC data end up on the CG laptop computer?	13
	C. Why wasn’t FEC data removed from the CG laptop computer?	16
	D. Who had access to the FEC data on the CG laptop computer?	20
	E. Why was FEC data released to the FCC/OIG?	22
	F. What data encryption and password controls did CG use to protect FEC data?	26
V.	Findings	30
VI.	Recommendations	30
VII.	Privacy Act and Freedom of Information Act Notice	31
	Attachment List	32

I. EXECUTIVE SUMMARY

On February 10, 2009, Kent Nilsson, the Inspector General (IG) for the Federal Communications Commission (FCC), contacted IG Lynne McFarland, to advise that his office received a laptop computer from Clifton Gunderson LLP (CG), which contained data of the Federal Election Commission (FEC). Clifton Gunderson LLP was a contractor to both the FCC Office of Inspector General (OIG) and the FEC OIG. Based on this information, the FEC Office of Inspector General immediately initiated an investigation to determine the circumstances surrounding the alleged release of FEC data.

The OIG investigation was initiated to determine whether CG improperly disclosed sensitive FEC information without authorization. The investigation was also conducted to determine whether CG violated the FEC's data security requirements, including: Directive 58 *Electronic Records, Software and Computer Usage*; Mobile Computing Security Policy (58-4.3), and FEC Non-Disclosure Agreements.

Based upon this investigation, the OIG determined that CG improperly released sensitive FEC data to the FCC without authorization. This unauthorized release was found to be accidental and limited only to the FCC OIG. CG also failed to report this accidental disclosure to the FEC OIG. It was further determined that CG failed to comply with the FEC's data security requirements. The OIG found that CG failed to remove FEC data from its laptop at the conclusion of the audit, and prior to the laptop's transfer to the FCC. The OIG also found that CG failed to install, within a timely manner, encryption software on this laptop.

The OIG conducted this investigation from February 10, through May 15, of 2009. Investigative activities conducted during this period included seventeen (17) witness interviews; three meetings with CG partners; three meetings at the FCC to examine the laptop's hard drive; a review of the 402 FEC data files; and a review of FEC OIG records pertaining to the CG contract and audit services. CG provided the OIG with full cooperation throughout the investigation.

The OIG staff met frequently with Alec Palmer, the Chief Information Officer (CIO), and Edward Bouling, the Information Systems Security Officer (ISSO), throughout the investigation. The OIG provided the CIO and ISSO with regular updates on investigative activities. The CIO and ISSO provided the OIG with technical subject matter assistance concerning data security requirements. It should also be noted that the OIG received technical assistance during the investigation from IT and computer forensic personnel at the FCC OIG.

Clifton Gunderson, LLP (CG) is a large certified public accounting (CPA) and consulting firm. CG audited the FEC's annual financial statements, on behalf of the OIG, during the fiscal years (FY) 2004 through 2008. For these audit services, the FEC paid contract costs to CG totaling \$492,314.79.

In 2004, CG signed the FEC contract, which contained a "Non-Disclosure of Confidential Data" provision. CG's partners and auditors also signed annual FEC Non-Disclosure Agreements and attended the FEC's mandatory computer security awareness training. This training explained the contractor's obligations under Directive 58 and the FEC's Mobile Computing Security Policy (58-4.3). CG also agreed to comply with FEC security requirements in a letter dated September 5, 2007, sent to the FEC's Chief Information Officer (CIO). The data security requirements that CG agreed to comply with included:

- Take reasonable precautions to protect against unauthorized disclosure of sensitive, protected, and confidential FEC information.
- Remove any and all FEC data from all laptops within 90 days of the conclusion of the audit (when the final report is issued).
- Encrypt all FEC data on all Clifton Gunderson laptops.
- Report immediately any instance of any and all irregularities, including unauthorized disclosures, concerning FEC data.

The FEC provided CG with a definition of "sensitive information," as defined under Directive 58, as "any data/information (whether in an electronic or non-electronic format), where loss, misuse, or unauthorized access to or modification of, could seriously hamper the Commission's ability to carry out its mandated functions."

The OIG investigation was conducted with a focus of determining answers to the following questions: 1) What FEC data was found on the laptop?; 2) How did FEC data end up on the CG laptop computer?; 3) Why wasn't FEC data removed from the CG laptop computer? 4) Who had access to the FEC data on the CG laptop computer?; 5) Why was FEC data released to the FCC/OIG?; and 6) What data encryption and password controls did CG use to protect FEC data? The results of these six questions are summarized below. The full details of the investigation and the findings are contained in the body of the report.

A. What FEC data was found on the CG laptop?

The investigation determined that 402 electronic files of FEC audit data were saved on the hard drive of a CG laptop computer. None of these files contained personally identifiable information (PII). The discovered FEC data consisted of CG's audit reports and workpapers from FEC financial statement audits conducted in the fiscal years (FY) 2006 and 2007.

The FEC CIO determined that several of the 402 electronic files included sensitive data concerning the FEC's Information Technology (IT) security program. This sensitive IT information included a network diagram, internet protocol (IP) addresses, server configurations and standards, and computer machine names.

B. How did FEC data end up on the CG laptop computer?

CG requested IT and financial information from the FEC for review in connection with the annual financial statement audits. The FEC furnished electronic copies of the requested documents in a shared folder on the FEC network. CG assigned a laptop computer to [REDACTED] an IT auditor, for use on the fiscal year (FY) 2007 FEC financial statement audit. CG installed an electronic document management program called FX Engagement on the laptop, and instructed [REDACTED] to save his audit reports and workpapers in the FX Engagement program.

[REDACTED] was unable to save his audit documents on the CG provided laptop, due to difficulties with the FX Engagement program. The FEC documents saved on the laptop assigned to [REDACTED] were downloaded to the laptop from CG's network server, using the FX Engagement program. [REDACTED] could not have downloaded the FEC documents to the laptop because he did not have access to CG's network server. CG did not give [REDACTED] access to CG's network server because [REDACTED] was a subcontractor. The investigation was unable to determine who on CG's staff, with access to the network server, could have downloaded the FEC documents to the laptop. No one on CG's staff admitted to downloading the FEC documents on to the CG laptop. The circumstances suggested that one of CG's audit managers, [REDACTED] or [REDACTED], were most likely responsible for downloading the FEC documents on to the laptop.

C. Why wasn't FEC data removed from the CG laptop computer?

CG was required under FEC policy to remove all FEC data from its laptop within 90 days of the close of the audit. The audit closed on November 13, 2007. CG failed to remove the FEC data from the laptop within the agreed upon 90 day period.

CG provided a number of reasons why the FEC data was not deleted from the laptop. First, CG indicated the deletion process was overlooked because the laptop was returned by a subcontractor. Second, CG reported that a breakdown in tracking the laptop on a sign in/sign out log prevented the laptop from being reimaged (properly prepared for reuse). Third, CG indicated that the FEC data was not removed because it was hidden on the hard drive when the folder containing the data was renamed and saved outside of the FX Engagement program. And finally, CG suggested the laptop was not reformatted before it was transferred to the FCC, because of an existing urgency to get a replacement laptop to the FCC.

D. Who had access to the FEC data on the CG laptop computer?

The investigation determined that the CG laptop remained in the custody of CG staff from the time it was used on the FEC audit, through the time it was given to the FCC OIG. From around June of 2007, through in or around August 2007, [REDACTED] had sole access to the laptop, while he performed his work on the FEC audit. [REDACTED] then returned the laptop to CG's audit manager [REDACTED], who returned it to the CG Calverton office. From August 2007, through March 2008, the laptop was apparently stored in a secure network equipment room in the Calverton office. In March 2008, CG employee [REDACTED], and CG partner [REDACTED], had access to the laptop.

From March 2008, through September 2008, the laptop was apparently stored in the secure network equipment room in CG's Calverton office. In September 2008, CG systems administrator [REDACTED] had access to the laptop. From September 2008, through February 2009, the laptop was apparently stored in the secure network equipment room in CG's Calverton office. In February 2009, CG employees [REDACTED] and [REDACTED] had access to the laptop. In February 2009, [REDACTED] gave the laptop to Roy Connor at the FCC OIG.

E. Why was FEC data released to the FCC/OIG?

The OIG investigated the circumstances, which led CG to give a laptop containing FEC data to the FCC. CG had a contract to perform an FCC audit on behalf of the FCC OIG. The investigation determined that the disclosure of FEC data was accidental. It was further determined that CG provided this laptop to the FCC OIG as a replacement, to resolve a problem that the FCC was having with a previous CG laptop. The previous laptop that CG gave to the FCC was apparently missing a software program needed to view CG's electronic audit workpapers.

The CG laptop that contained the FEC files was randomly selected as the replacement laptop for the FCC, without knowledge of the FEC data it stored. Prior to the laptop's transfer to the FCC OIG, CG auditor [REDACTED] manually inspected and removed data that was stored in the recycle bin and the FX Engagement program. [REDACTED] was unaware that a folder containing FEC data was stored on the laptop because it was saved in a renamed folder on the C: drive. According to CG, due to the urgency of the FCC OIG request, CG did not reformat the laptop before transferring it to the FCC.

FCC OIG Audit Director Roy Connor discovered the FEC data on the laptop on Thursday, February 5, 2009. Roy Connor reported it to CG on Friday, February 6, 2009, at 3:50 pm. At 4:30 pm, on Friday, February 6th, Roy Connor told CG IT partner, [REDACTED], that he discovered FEC data on the laptop. CG never notified the FEC of the unauthorized disclosure. The FEC OIG contacted CG regarding the disclosures on February 10, 2009.

CG partner [REDACTED] said he didn't notify the FEC of the data release because Roy Connor did not provide enough information about the incident and [REDACTED] wanted to better understand the situation. CG partner [REDACTED] reported that CG did file an internal incident report to document the release on Saturday, February 7th.

F. What data encryption and password controls did CG use to protect FEC data?

On September 5, 2007, CG partner [REDACTED] gave assurances to the FEC in writing that CG would encrypt all FEC data on CG laptops. The OIG investigation revealed that CG did not install its encryption software (Pointsec) on the laptop containing FEC data until March 8, 2008, at 10:32 am. The installation of this encryption software occurred four months after the completion of the 2007 FEC audit.

The OIG investigation revealed that CG had password protections on its laptops; however, on three or four occasions, CG staff reportedly wrote user names and passwords on laptops, in connection with Federal audits. First, when the laptop was issued to [REDACTED], CG reportedly placed a post-it note with a user name and password on the CG laptop. Second, CG auditor [REDACTED] placed a post-it note with a user name on the CG laptop assigned to Roy Connor. [REDACTED] later wrote the password to the computer on the same post-it note in Roy Connor's office. And finally, Roy Connor advised that CG gave laptops to FCC OIG employees, Sophie Jones and Sharon Spencer, with user names and passwords on attached post-it notes.

Summary of Findings

The OIG found reasonable cause to believe that CG failed to comply with FEC's data security requirements. These findings include:

- CG disclosed sensitive FEC information to the FCC OIG without authorization. However, this unauthorized disclosure appeared accidental and limited only to the FCC OIG.
- CG failed to take reasonable precautions to protect FEC data against unauthorized disclosure. The laptop used on the FEC audit was not reformatted or reimaged prior to transfer to a new client.
- CG failed to remove FEC data from its laptop, as agreed, within 90 days of the conclusion of the audit. The audit concluded on November 13, 2007. The FEC data remained on the laptop long after the 90 day deadline of February 2008.
- CG failed to encrypt FEC data on its laptop within a timely manner. The encryption software "Pointsec" was not installed on the CG laptop until March 8, 2008. This was long after CG's partner agreed to install encryption software on September 5, 2007.

- CG failed to report to the FEC OIG the unauthorized disclosure of FEC data. CG partner [REDACTED] learned of the data release on Friday, February 6, 2009, at 4:30 pm. [REDACTED] failed to call the FEC to report the incident, on that Friday, or on the following Monday.

Summary of Recommendations

The OIG has offered three suggestions to the FEC to improve the protection of sensitive FEC data. These include: 1) incorporate contractor data security standards in all FEC contracts; 2) require post-contract certifications that FEC data has been removed from all laptops; and 3) improve the identification of FEC data that is, or should be, classified as “sensitive.”

As a result of this incident, the OIG implemented a new policy entitled “FEC OIG Contractor Security Standards,” to strengthen data security controls on all future OIG audit contracts. The new OIG policy was presented to the FEC CIO for consideration on all FEC contracts. Also, as a result of this incident, the FEC CIO and ISSO drafted new “Minimum Contractor System Security Standards,” to be incorporated into future FEC contracts. The OIG has already incorporated the new contract language prepared by the CIO and ISSO into the OIG’s new financial statement audit contract signed in April 2009.

II. ALLEGATION

Clifton Gunderson LLP, a former FEC contractor, allegedly disclosed sensitive FEC data to another federal agency, the Federal Communications Commission (FCC), without authorization, in violation of Directive #58 and FEC Non-Disclosure Agreements.

III. BACKGROUND

Clifton Gunderson (CG) is a large certified public accounting (CPA) and consulting firm, with over 1600 employees and 45 offices, in fourteen states and Washington DC. The firm’s federal government practice has provided audit services to approximately 26 federal agencies, including the FEC and FCC. These services have included financial statement audits required under the Chief Financial Officers (CFO) Act. CG’s office that serviced the FEC is located at 11710 Beltsville Drive, Suite 300, Calverton, MD 20705. CG’s local telephone number is (301) 931-2050. [REDACTED] is the partner-in-charge of CG’s federal government practice. [REDACTED] is the partner-in-charge of CG’s Calverton office.

A. FEC Contract No. FE4AC0065: Financial Statement Audit

On February 25, 2004, the FEC awarded a contract to CG to audit the FEC's annual financial statements, on behalf of the OIG, as required under the Accountability of Tax Dollars Act of 2002 (Public Law 107-289). The contract number for this award is "GS23F0135L" (purchase order number FE4AC0065). This contract included four option renewal periods for the subsequent years of 2005 through 2008. All four option years were exercised based on CG's performance. The contract cost, including option years and modifications, totaled approximately \$492,314.79.

On February 24, 2004, CG partner [REDACTED] signed the FEC audit services contract (FE4AC0065) on behalf of CG. This contract contained a "Non-Disclosure of Confidential Data" provision, which was incorporated into the contract as part of the Statement of Work (SOW). The "Non-Disclosure" provision expressly required that "[t]he contractor...shall not... reveal the nature or content of any [nonpublic] FEC information." (Attachment 1)

B. CG Staff Assigned to the FEC Contract

In 2007, CG had two principal partners who oversaw the audit on the FEC contract. These partners were [REDACTED] and [REDACTED]. [REDACTED] oversaw the information technology (IT) systems portion of the FEC audit. [REDACTED], who was the partner-in-charge of the 2007 FEC audit, oversaw the financial statement portion of the audit.

[REDACTED] is the partner-in-charge of the Calverton office and he was the concurring partner on the FEC audit. In addition, [REDACTED] oversaw equipment controls and administrative functions, which supported the audits.

During the 2007 financial statement audit, CG assigned five auditors to work on the FEC contract. These five auditors included two senior managers, [REDACTED] and [REDACTED]. Senior audit manager [REDACTED] supervised two auditors (Rebecca Collier and Andre Reid), who performed the financial statement portion of the FEC audit. [REDACTED] reported to CG partner [REDACTED].

Senior audit manager [REDACTED] reported to CG partner [REDACTED]. [REDACTED] supervised one auditor, [REDACTED] who conducted the IT systems portion of the FEC audit. [REDACTED] was a consultant subcontracted by CG to work on the FEC audit. [REDACTED] is a certified information systems auditor (CISA). [REDACTED] is employed by a company called Samlin Consulting. As a subcontractor for CG, [REDACTED] also reported to his employer, [REDACTED], who is the owner of [REDACTED] Consulting.

C. CG's End User Support and Administrative Staff

CG has an internal information technology (IT) support group known as "End User Support," located in Timonium, Maryland. This IT support group is run by [REDACTED], who is one of CG's systems administrators. [REDACTED] supervised another IT support employee in End User Support, [REDACTED]. CG's End User Support group was responsible for IT related support, including the purchase, inventory, and disposal of computers and network equipment; computer configurations and formatting; software installations and updates; data security and removal; and network related support.

[REDACTED] and [REDACTED] had responsibility for installing computer software programs and configuring laptops for client and/or subcontractor use. Once a laptop was configured, a label or sticky note was placed on it to show which client or subcontractor the laptop was intended for. Once the laptops were prepared for use, [REDACTED] or [REDACTED] brought them to the Calverton office to be stored in a secure computer network room until needed.

The computer network room in the Calverton office stored assigned laptops and "loaner pool" laptops. The loaner pool laptops were spares available for either in-house use by CG employees, or for use by clients or subcontractors. Many of the laptops stored in the computer network room were either waiting to be taken to a client or had been returned by a client.

[REDACTED] performed inventory inspections to account for computers and equipment stored in the network room. [REDACTED] or [REDACTED] frequently brought new laptops to the Calverton office in person and showed new users how to login. [REDACTED] often came down to the Calverton office and cleaned client data from the laptops after their use. [REDACTED] would then place a label marked "spare" on the returned laptops that he cleaned. [REDACTED] was the custodian of the computer equipment.

Access to CG's computer network room in the Calverton office was controlled by a small grey electronic security token key known as "FOB" key, which was scanned using a card reader. No one without an access key could gain entry into the network room. CG was questioned by the OIG on the security of the network room and no break-in incidents involving the network room were reported. Besides [REDACTED] and [REDACTED] three administrative staff employees in the Calverton office had access to the network room. These employees were [REDACTED], [REDACTED] and [REDACTED] and [REDACTED] reported to [REDACTED], who reported to CG's partner [REDACTED].

When an auditor returned a laptop after use, it was typically given to [REDACTED] or some other administrative staff, who would note the return of the laptop on an equipment checkout log, and then secure the computer in the network room. [REDACTED] was hired by CG in 2008.

In 2007, [REDACTED] predecessor, [REDACTED] was the administrative assistant who maintained the equipment checkout log on equipment checked in and out of the computer network room.

D. FEC Directive 58 & Computer Security Training

The FEC required CG's partners and auditors, who were involved with the 2007 and 2008 financial statement audits, to complete the FEC's mandatory computer security awareness training. The FEC also required signed written statements acknowledging that each CG employee completed the computer security awareness training. This computer security training consisted of a PowerPoint presentation entitled "FEC's Information System Security Awareness Program." The training covered FEC Commission Directive 58: *Electronic Records, Software and Computer Usage*, which applied to both FEC staff and contractors. Directive 58 required each user to erase and/or destroy sensitive information the user chose to store outside of the FEC network. Directive 58 defined "sensitive information" as "any data/information (whether in an electronic or non-electronic format), where loss, misuse, or unauthorized access to or modification of, could seriously hamper the Commission's ability to carry out its mandated functions." (Attachments 2 and 3)

The FEC computer security awareness training also covered the FEC Mobile Computing Security Policy, Policy Number 58-4.3. Under sections 2(j) and (k), all laptops that access the FEC local area network (LAN) were required to be encrypted and have a two-factor authentication mechanism. (Attachment 4)

E. FEC Non-Disclosure Agreements

On March 9, 2007, in preparation for the fiscal year (FY) 2007 financial statement audit, Dorothy Maddox-Holland (HOLLAND), Special Assistant to the IG, sent an email to CG's audit manager [REDACTED], requesting that CG staff sign an FEC Non-Disclosure Agreement. On this agreement, each of CG's auditors and partners certified that they "will not disclose any non-public information to any... non-contractor personnel..." CG's partners and auditors further certified that they understood that this "prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work." A signed FEC "Non-Disclosure Agreement" was obtained from CG partners [REDACTED], [REDACTED], and [REDACTED]. It was also signed by CG auditors [REDACTED], [REDACTED], [REDACTED], and others. (Attachment 5)

In connection with the FY 2008 financial statement audit, CG's partners and auditors signed an FEC "Non-Disclosure Agreement for Contractors." This agreement was signed in May 2008, by CG partners [REDACTED] and [REDACTED]. It was also signed by CG auditors [REDACTED], [REDACTED], [REDACTED], and others. (Attachment 6)

Each CG auditor and partner who signed the “Non-Disclosure Agreement for Contractors” agreed to “... take all reasonable precautions to protect against... unauthorized disclosure of such [sensitive, protected, and confidential] information...” CG staff also agreed “to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information...” (Attachment 6)

F. CG Assurances to Secure Sensitive FEC Data

To comply with new requirements under the FEC Mobile Computing Security Policy (Number 58-4.3), including encryption requirements, the FEC requested written security assurances from CG. IG Special Assistant HOLLAND sent an email on March 9, 2007, to CG’s audit manager [REDACTED], requesting an acknowledgement on company letterhead that “the FEC’s sensitive data is and will be secure.” This request was made as a result of software incompatibility issues, and an inability to install the FEC’s encryption technology on CG’s laptops, HOLLAND made the request to CG on behalf of Edward Bouling (BOULING), the FEC Information Systems Security Officer (ISSO). [REDACTED] responded in an email dated March 13, 2007, in which she requested clarification of the terms “sensitive” and “secure.”

On March 13, 2007, BOULING sent an email to CG’s audit manager [REDACTED], in which he defined “sensitive information” as defined in FEC Directive 58: “any data/information (whether in an electronic or non-electronic format), where loss, misuse, or unauthorized access to or modification of, could seriously hamper the Commission’s ability to carry out its mandated functions...”

In his March 13th email, BOULING provided CG with examples of sensitive information, which included “descriptions of FEC Information Resources” and “[d]escriptions of procedures and policies used to protect our network and information resources.” BOULING’s March 13th email to CG further stated that the FEC “need[s] some type of assurance that the sensitive information your auditors access remotely or remove from our premises are adequately protected.”

On March 27, 2007, HOLLAND contacted BOULING by email to obtain clarification of the FEC’s encryption requirements for CG’s laptops. On April 26, 2007, HOLLAND sent an email to BOULING for guidance on verifying whether or not CG’s computers met the FEC’s criteria for securing sensitive data. In an email dated May 1st, BOULING responded to HOLLAND, stating that CG was required to provide “a statement on company letterhead (from someone in authority)” that included, among other things, that any “FEC data downloaded or copied to a Non-FEC machine will be encrypted” and that data will be “removed from all Non-FEC machines no later than 90 days of the audit’s conclusion.”

HOLLAND forwarded BOULING's email, dated May 1st, to CG's audit manager [REDACTED]. In response to BOULING's request, on September 5, 2007, CG's partner [REDACTED] sent a letter on company letterhead to Alec Palmer, the FEC's Chief Information Officer (CIO). In this letter, [REDACTED] requested an exception to the FEC's policy [# 58-4.3] that required a two-factor authentication on laptops storing sensitive FEC information. In connection with his request for an exception, [REDACTED] advised in his letter to the CIO that CG:

- Will remove any and all FEC data from all laptops within 90 days of the conclusion of the audit (when the final report is issued).
- Will encrypt all FEC data on all Clifton Gunderson laptops.
- Will report any instance of any and all irregularities concerning FEC data immediately. (Attachment 7)

IV. INVESTIGATION DETAILS

A. What FEC data was found on the CG laptop?

Answer Summary: A folder containing approximately 402 electronic files was saved to the C: drive on the CG laptop computer. No personally identifiable information (PII) was found within these files. The documents consisted of CG's audit reports and workpapers related to the FY 2006 and FY 2007 FEC financial statement audits. Several of the 402 files contained sensitive IT security program information and nonpublic financial information. The sensitive IT information included a computer network diagram, internet protocol (IP) addresses, and server configurations.

On February 10, 2009, Kent Nilsson, the Inspector General (IG) of the Federal Communications Commission (FCC), contacted IG Lynne McFarland to advise that his office received a laptop computer from Clifton Gunderson, LLP (CG), which contained data of the Federal Election Commission (FEC). That same day, Jon Hatfield (HATFIELD), Deputy IG, and BOULING, the FEC ISSO, went to the FCC and met with Roy Connor (CONNOR), Director of IS Audit for the FCC/OIG, to determine what FEC data was found. During this meeting, CONNOR provided HATFIELD a copy of an electronic folder named "Pfxengagement.old," which contained approximately 402 files of FEC data.

On that same day, February 10th, the OIG reviewed the 402 files received from the FCC OIG, to determine whether or not any of the documents contained personally identifiable information (PII). No PII was found within the documents reviewed. However, this review identified several documents that were determined by the Chief Information Officer (CIO) to be nonpublic and sensitive FEC information.

The FEC data found on CG's laptop included some of CG's workpapers and audit reports from the FEC financial statement audits conducted in fiscal years (FY) 2006 and 2007. These audit workpapers included several sensitive FEC provided documents, such as an information technology (IT) network diagram, internet protocol (IP) addresses, server configurations and standards, machine names, and "work reports" on FEC employees. On February 11, 2009, the OIG provided a copy of the electronic files found on the CG laptop computer to ISSO Edward Bouling (BOULING), for further review.

The OIG interviewed CONNOR during the investigation to determine the events which led to his discovery of FEC data. CONNOR advised:

On February 3, 2009, he received a laptop from [REDACTED] a CG auditor who worked on the FCC contract. This CG laptop computer was given to CONNOR for the purpose of reviewing electronic workpapers related to an FCC audit. Two days later, on February 5th, CONNOR discovered approximately 402 electronic files in a folder on the laptop, which pertained to a 2007 FEC audit.

On Friday, February 6, 2009, at 3:50 pm, CONNOR reported his discovery of the FEC data to CG auditor [REDACTED]. That same day, Friday, at 4:30 pm, he received a call from CG partner [REDACTED]. During this conversation, CONNOR informed [REDACTED] that he discovered FEC audit data on the laptop that CG provided to him.

After CONNOR notified [REDACTED] about the FEC data he discovered, [REDACTED] told CONNOR he wanted to pick up the CG laptop with the FEC data and switch it for the original laptop that was meant for the FCC. On Monday, February 9, 2009, [REDACTED] called CONNOR and she scheduled a time to come out to the FCC on February 10th, to switch out the laptops.

During the OIG investigation, [REDACTED] CG's IT partner, was questioned as to why he didn't notify the FEC as soon as he learned that the FCC found FEC data on a CG laptop. In response, [REDACTED] advised the following:

[REDACTED] didn't notify the FEC because, at the time, he had no idea what FEC data was found on the laptop. [REDACTED] said he wanted to get the laptop and see what data Roy Connor at the FCC was talking about; so that [REDACTED] could evaluate whether notifications were needed. [REDACTED] wanted to be in a position to describe to the FEC what data was released before he notified the client. Roy CONNOR at the FCC was not forthcoming to [REDACTED] about the specific type of data CONNOR found on the laptop. CONNOR did not specify where the FEC data was found on the computer. CONNOR was a little vague and evasive about the FEC data he found. [REDACTED] felt it was premature to notify the FEC that Friday or Monday until CG could see what data was released.

B. How did FEC data end up on the CG laptop computer?

Answer Summary: CG requested IT and financial information from the FEC for review in connection with the annual financial statement audits. The FEC furnished electronic copies of the requested documents in a shared folder on the FEC network. CG assigned a laptop computer to [REDACTED], an IT auditor, for use on the fiscal year (FY) 2007 FEC financial statement audit. CG installed an electronic document management program called FX Engagement on the laptop, and instructed [REDACTED] to save his audit reports and workpapers in the FX Engagement program.

[REDACTED] was unable to save his audit documents on the CG provided laptop, due to difficulties with the FX Engagement program. The FEC documents saved on the laptop assigned to [REDACTED] were downloaded to the laptop from CG's network server, using the FX Engagement program. [REDACTED] could not have downloaded the FEC documents to the laptop because he did not have access to CG's network server. CG did not give [REDACTED] access to CG's network server because [REDACTED] was a subcontractor. The investigation was unable to determine who on CG's staff, with access to the network server, could have downloaded the FEC documents to the laptop. No one on CG's staff admitted to downloading the FEC documents on to the CG laptop. The circumstances suggested that one of CG's audit managers, [REDACTED] or [REDACTED], were most likely responsible for downloading the FEC documents on to the laptop.

In May 2007, CG requested FEC information for review, in connection with the annual financial statement audit. This information consisted of both sensitive IT documents and nonpublic financial documents concerning FEC operations. CG requested the FEC documents using "Provided By Client (PBC)" lists, during the preliminary preparation phase and throughout the audit. In June 2007, the FEC furnished to CG electronic copies of the requested PBC documents by saving them to a shared drive on the FEC server.

The IT documents provided to CG contained information concerning the FEC's security program, to include access controls, change controls, system software, and service continuity. The financial documents provided to CG contained information concerning the FEC's general operations, financial reporting, Fund Balance with Treasury, and property, plant and equipment (PP&E).

In April 2007, CG assigned the laptop that was later found to contain the FEC data to [REDACTED]. This laptop was a Hewlett Packard (HP) computer with a serial number "2UA508087J." (Attachment 8) During the OIG investigation, a hard drive image of the laptop was examined to identify users and activities on the computer. This examination was conducted at the FCC OIG, using a computer forensic software program.

The computer hard drive image examination revealed that on April 9, 2007, [REDACTED], who works in CG's End User Support, accessed the laptop and performed the following:

- [REDACTED] reformatted and reimaged the laptop computer's hard drive;
- At 4:43 pm, he created his own user profile ("[REDACTED]6274") for the computer; and
- At 5:15 pm, he installed the FX Engagement program on the computer. This installation also created the electronic folder where the FEC data was ultimately found.¹

"FX Engagement" is a computer software program that allowed CG to manage and store electronic workpapers in connection with their audits. CG first used the FX Engagement program on the financial portion of the FEC audit in FY 2006. In the following year, FY 2007, CG fully implemented the FX Engagement program on the FEC audit, which also included the IT portion of the audit.

On April 19, 2007, CG's End User Support staff [REDACTED] or [REDACTED] created a user profile on the laptop (0000[REDACTED] for use by [REDACTED]), an IT auditor. The request for a CG laptop for [REDACTED] was made by CG's IT audit manager [REDACTED]. In or around June 2007, End User Support furnished the laptop computer to CG's Calverton office for [REDACTED]'s use. (Attachment 9)

The OIG interviewed [REDACTED] during the investigation to determine his use and activities on the laptop during the 2007 FEC audit. [REDACTED] advised that he carried the CG issued laptop around with him during the 2007 FEC audit, but that he did not use it. [REDACTED] kept the laptop in his possession from around June 2007, to sometime in August 2007. He did not recall specifically the time period he kept the laptop. [REDACTED] advised that FEC audit documents from 2006 were already loaded into the FX Engagement program when he first received the laptop from CG's audit manager, [REDACTED]. CG did not give [REDACTED] access to CG's network server so, therefore, [REDACTED] was unable to download or save FEC files to the laptop, from the CG server.

According to [REDACTED], he did not use the CG laptop to perform his work during the 2007 FEC audit. [REDACTED] said he performed his audit work on his Samlin issued laptop. [REDACTED] further advised:

¹ CG partners [REDACTED] and [REDACTED] advised that [REDACTED] would not have loaded FEC documents on the laptop during the installation process of FX Engagement. FEC documents would have been loaded into the FX Engagement folder by an auditor after [REDACTED] installed the program.

The CG laptop was issued to him so he could store electronic workpapers into the FX Engagement program. He had never used FX Engagement before and was unable to load any documents into the program on the laptop.

██████ never saved or downloaded any FEC documents or audit workpapers on the CG laptop. He used his Samlin issued laptop to perform all of his audit work because it had the necessary virtual private network (VPN) and Visio flowcharting software programs installed.

During the audit, ██████ unsuccessfully attempted to load one of his 2007 audit documents, an “access control workpaper,” into the FX Engagement program on the CG laptop. ██████ was unable to remove the prior year’s audit documents whenever he tried to load the 2007 document. These preloaded 2006 audit documents prevented him from uploading his 2007 audit workpapers on to the CG laptop.

He did not know who saved or downloaded the 402 files that were found in a FX Engagement folder to the CG laptop. He thought the 2006 audit documents were probably loaded on the computer by CG’s end user staff, or by ██████, who gave him the laptop. ██████ could not have downloaded any FEC documents from CG’s network server since he was never given access to the CG network. He believed CG did not give him access to the CG network because he was a subcontractor.

Since ██████ was unable to load his documents on to the CG laptop, he and ██████ agreed that ██████ would email his audit workpapers and documents, in password protected zip files, to ██████ CG’s audit manager. ██████ then uploaded the audit documents into the FX Engagement program. ██████ returned the CG laptop to ██████ after his failed attempts to load his documents into FX Engagement.

During the investigation, the OIG reviewed the files found on the CG laptop in a folder named “Pfxengagement.” This review confirmed that the FEC documents included audit workpapers from FEC audits in both FY 2006 and FY 2007. The “last modified” dates for these electronic files ranged from December 2, 2005, through August 17, 2007. The last document saved to the folder was an FX Engagement generated document called a “Synchronization History Log,” which was dated August 17, 2007.

The OIG interviewed ██████, CG’s systems administrator, regarding the “Synchronization History Log,” dated August 17, 2007. ██████ advised that the FX Engagement program installed on the CG laptop generated this document because on August 17th, someone created a “binder package” on this laptop. This “binder package” was created within the FX Engagement program to store audit documents.

On February 11, 2009, CG assigned one of its senior managers, [REDACTED] an IT auditor from Mechanicsburg, PA, to conduct an internal investigation of the laptop issue. The OIG requested that [REDACTED] and CG prepare an investigative report to document [REDACTED]'s investigative findings. (Attachment 9)

During the investigation, [REDACTED] was questioned by the OIG about the FX Engagement binder package created on August 17, 2007. He advised that the "binder package was received by the computer ID assigned to [REDACTED]." Further, [REDACTED] could not say for certain whether it was [REDACTED] or a CG auditor who created the binder package. In the CG report, [REDACTED] wrote:

"Binder packages can also be created from within FX, which will create local copies of files. This functionality is utilized and needed in situations whereby the audit teams do not receive internet/network access at the clients they are working at. Further, there is peer-to-peer synchronization capability, for users to connect machines directly to copy/synch data. Data may also be copied via binder packages sent through email or via USB drive or CD, but would need to be loaded into FX to be accessible." (Attachment 9)

On page 21 of the CG report, [REDACTED] reported the results of his interview with CG's End User Support staff. With regards to synchronization, [REDACTED] wrote:

"The subcontractor [REDACTED] was not provided with a CG network ID. Therefore, he [REDACTED] would not have been able to upload/synch data to FX centrally. He would have needed to sync via a peer-to-peer connection with another person's laptop, or transferred files via email or CD. It is believed this may have taken place between IT Audit Manager [REDACTED] and the subcontractor [REDACTED]. (Attachment 9)

The OIG interviewed CG's audit manager [REDACTED] regarding his supervision of [REDACTED] and the IT portion of the 2007 FEC audit. [REDACTED] was questioned about his role in the process to upload [REDACTED]'s work documents into the FX Engagement program. [REDACTED] could not recall how the documents were loaded into FX Engagement.

None of the auditors who worked on the FEC contract admitted to downloading the FEC documents on to the CG laptop assigned to [REDACTED]. Since [REDACTED] did not have access to CG's server, the circumstances suggested that one of the audit managers, [REDACTED] or [REDACTED], probably downloaded the documents to the laptop.

C. Why wasn't FEC data removed from the CG laptop computer?

Answer Summary: CG provided a number of reasons for not deleting the FEC data off of the laptop. First, the deletion process was overlooked because the laptop was returned by a subcontractor. Second, a breakdown in tracking the laptop on sign-in/sign-

out logs prevented the laptop from being reimaged. Third, the renaming of the folder that contained the FEC data, and the saving of the folder outside the FX Engagement program, prevented its removal. And finally, the FCC's urgent need for a temporary laptop led to the laptop's transfer to a new client, without first reformatting it.

CG agreed to remove any and all FEC data from all laptops within 90 days of the conclusion of the 2007 audit. CG's IT partner [REDACTED] communicated this in a letter dated September 5, 2007, to the FEC CIO Alec PALMER. In this letter, [REDACTED] specified that the "conclusion of the audit" shall mean the date when the final report was issued. CG's final audit report was issued on, and dated, November 13, 2007. Therefore, in accordance with [REDACTED]'s letter, CG agreed to remove FEC data from its laptops by mid-February 2008. (Attachment 7)

[REDACTED] completed his FEC audit work sometime before October 1, 2007. [REDACTED] believed he may have returned his CG laptop to audit manager [REDACTED] before August 17, 2007. When [REDACTED] was interviewed by the OIG, she did not specifically recall receiving the laptop from [REDACTED]. However, [REDACTED] indicated she had no reason to doubt that [REDACTED] returned the CG laptop to her. [REDACTED] advised that if she received a laptop from [REDACTED] she would have given the laptop to the administrative staff at the Calverton office, to lock up in the computer network room. A review of CG's equipment checkout log revealed that no entry was logged to document the return of [REDACTED]'s laptop.² (Attachment 8)

CG's senior auditor [REDACTED] investigated the incident for CG to determine why the FEC data was never removed from [REDACTED] laptop. In the CG report, [REDACTED] provided a number of explanations as to why CG failed to remove the FEC data, which included the following:

- Page 9 of the CG report: CG's engagement partner notifies "all team members to remove/delete all related data from their... local copies of FX binders" after the partner finalized his/her review. It appeared the process to delete data was "overlooked" in this case, because the CG laptop was "returned from a subcontractor at the time the binder [workpapers for the audit] was finalized."³
- Page 9: CG's Service Operations office did not follow CG procedures to reimage the laptop (thereby deleting the data) because CG staff did not enforce its "sign-in/sign-out

² In 2007, [REDACTED], former CG administrative assistant, maintained the equipment checkout log for CG's computer network room in the Calverton office. She is no longer a CG employee and was not interviewed during the OIG investigation.

³ Investigator's Note: The CG report was silent as to who was responsible and overlooked the process to delete data on [REDACTED] laptop after the binder was finalized.

controls” and did not follow “procedures to log machines being removed from or returned to the loaner pools.” The laptop was returned to CG in early October, but was not registered on the sign-in/sign-out log when it was returned.

- Page 11: The failure to reformat the CG laptop, when it was transferred, was the result of a “breakdown in tracking,” which included “other times at which this machine was used for various reasons in 2008, and the machine was not logged in or out on the tracking sheet, or the sign-out log in Calverton.”
- Page 8: CG only ran KillDisk [computer software program to permanently delete data] for disposal of laptops, and [CG] reformatted drive[s] only during transfer of laptop to another employee (not necessarily if kept in loaner pool).⁴ (Attachment 9)

During the OIG investigation, the hard drive image of the computer was examined to determine the activities of various users on the CG laptop. This examination showed that in March 2008, CG’s End User Support staff accessed the CG laptop on three occasions and failed to delete the FEC data. CG’s End User Support is responsible for deleting client data from laptops and reimaging/reformatting laptops upon transfer to new users. The hard drive image review showed End User Support accessed the CG laptop on the following three occasions:

- On March 8, 2008, CG’s End User Support accessed the laptop and installed Pointsec encryption software.
- On March 12, 2008, ██████████, in CG’s End User Support, accessed the laptop and moved the folder that contained the FEC documents out of the FX Engagement program, by renaming it to “Pfxengagement.old” and saving it to the C:drive on the laptop. After ██████████ saved the folder containing FEC data to the C: drive, he then reinstalled the FX Engagement program on the laptop.
- On March 19, 2008, at 10:59 am, End User Support created a user profile “████████r2549” for CG’s partner-in-charge, ██████████, to have access to the CG laptop. ██████████ used the CG laptop on March 21, 2008, in connection with a slide show training presentation on federal sector audits.

The OIG investigation was unable to determine the reason ██████████ took steps on March 12, 2008, to keep the FEC data on the CG laptop, instead of deleting it. ██████████’s supervisor

⁴ Investigator’s Note: The CG report was unclear as to whether ██████████ laptop was placed into a “loaner pool” to be reassigned to a new user; or whether the laptop was reserved for ██████████ in the computer network room for use on the 2008 FEC audit.

██████████ was interviewed and advised that ██████████ probably renamed the folder, and saved it to the “C: drive,” to preserve the FEC data during a reinstallation of the FX Engagement program.

██████████ was able to conclude that it was ██████████ who renamed the folder containing FEC data by reviewing the data path for the FX Engagement program installed on the CG laptop. This data path showed the existing FX Engagement program on the CG laptop was reinstalled, under ██████████ user profile, on March 12, 2008.

On page 9 of the CG report, ██████████ made similar observations regarding the impact of ██████████ decision to rename the folder that contained the FEC data; and to save this data on the laptop’s hard drive outside of the FX Engagement program. ██████████ wrote:

Apparently, in March 2008, FX was reinstalled on the laptop. At that time, it seems that the prior FX directory(ies) were renamed to “Pfx Engagemen.old.” The “.old” portion is not standard naming convention, and would likely have been done in order to preserve prior FX data during the reinstall. This directory was never later removed or deleted. This created additional factors, as during the transfer of this laptop to the FCC OIG, Service Operations did instruct the IT Senior on how to remove all FX data, which was performed. However, again, since the data was now in a renamed folder/directory, the process to remove FX data was not successful, as it removed data from the “Pfx Engagement” directory, and not the folder which had been renamed to “.old.”
(Attachment 9)

During the investigation, ██████████ was interviewed about his March 2008 decision to rename the folder on the laptop that contained FEC data. ██████████ advised that he did not recall renaming this folder. ██████████ said that he has renamed folders using the “.old” label in the past, and he would have saved the FEC data on the hard drive if someone asked him to save it.

CG partner ██████████ was asked if he instructed ██████████ to preserve the FEC data on ██████████ laptop. ██████████ advised:

He did not recall ██████████ specifically asking him whether the FEC data on the laptop needed to be saved. If he was asked, ██████████ may have told ██████████ to preserve the data so that ██████████ would have it on the computer when he worked on the next year’s FEC audit. ██████████ may have been reinstalling the FX Engagement software on the laptop in March 2008, because a new version of FX Engagement was installed on all laptops.

On page 11 of the CG report, ██████████ explained why the CG laptop used on the FEC audit was never reimaged or reformatted before it was transferred to a new client, the FCC. ██████████ wrote:

Perhaps as a result of a contentious email from the FCC OIG, partners made determination to proceed and use a “pool” laptop in order to expedite the [FCC] OIG request for a new machine to review working papers.

The laptop was not directly reviewed by Service Operations and wasn't reformatted before providing to the FCC; although Service Operations was consulted via phone in setting up the machine. (Attachment 9)

D. Who had access to the FEC data on the CG laptop computer?

Answer Summary: From around June 2007, through in or around August 2007, [REDACTED] had sole access to the laptop, to perform his work on the FEC audit. In August 2007, [REDACTED] received the laptop from [REDACTED] and turned it in to CG's network equipment room. From August 2007, through March 2008, the laptop was apparently stored in a secure network equipment room in CG's Calverton office. In March 2008, CG employee [REDACTED] and partner [REDACTED] had access to the laptop.

From March 2008, through September 2008, the laptop was apparently stored in the secure network equipment room in CG's Calverton office. In September 2008, CG systems administrator [REDACTED] had access to the laptop. From September 2008, through February 2009, the laptop was apparently stored in the secure network equipment room in CG's Calverton office. In February 2009, CG employees [REDACTED] and [REDACTED] had access to the laptop. In February 2009, [REDACTED] gave the laptop to the FCC. The laptop has remained in FCC OIG custody pending the completion of the OIG's investigation.

The CG laptop in question (serial number 2UA508087J) was purchased on March 7, 2005. On April 9, 2007, [REDACTED], who works in CG's End User Support, reformatted and reimaged this laptop for transfer to a new user. On April 19, 2007, [REDACTED] created a user profile (“0000 [REDACTED]”) so that CG subcontractor Evans [REDACTED] could access the computer for use on the FEC audit. On this same day, April 19th, [REDACTED] installed the Fx Engagement program. [REDACTED] delivered the laptop to CG's Calverton office for [REDACTED]'s use. In or around June 2007, CG audit manager [REDACTED] gave the laptop to [REDACTED] at the FEC. (Attachments 8 and 9)

[REDACTED] kept the laptop in his possession from around June 2007, through in or around August 2007. [REDACTED] then returned the laptop to [REDACTED]. When interviewed by the OIG, [REDACTED] did not specifically recall receiving the laptop from [REDACTED]. She advised that if [REDACTED] returned his CG laptop to her, [REDACTED] probably gave it to the administrative staff in the Calverton office; so that it could be secured in the computer room. [REDACTED] did not have direct access to the computer room in the Calverton office.

In late September 2007, [REDACTED], a former CG administrative assistant in the Calverton office, had direct access to the computer equipment room. During that time period, [REDACTED] kept a "Wireless Equipment Checkout" log on equipment that was checked in and out of the equipment room. However, a review of this wireless equipment checkout log found no entry to show the laptop was returned to the Calverton equipment room. (Attachment 8)

On page 13 of the CG report, [REDACTED] reported that the laptop was returned to CG in early October 2007 and "presumably returned to the DC Computer Storage Room." (Attachment 9) The OIG reviewed the user profile data on the hard drive of the CG laptop with the assistance of an FCC-OIG Forensic IT Specialist. This review showed no activity on the computer from October 2007, through March 2008. This review showed that on March 8, 2008, at 10:32am, CG's End User Support staff installed encryption software known as "Pointsec" on the CG laptop. It also showed that on March 12, 2008, [REDACTED] installed updates on the CG laptop using a software program manufactured by Alltiris.

[REDACTED] software installation activity on the CG laptop, in March 2008, suggested that the laptop computer had remained in CG's custody during the previous six months; since the time that [REDACTED] returned the laptop to [REDACTED] in September 2007. Although CG never recorded the laptop on its equipment checkout log, the circumstances suggested that CG retained custody of it through the period when [REDACTED] accessed the computer to install programs in March 2008. This was further supported by the fact that no user profile activity was identified on the hard drive during the six months prior to March 2008. Also, there were no incidents of laptop theft or misuse reported by CG during this six month period. (Attachment 9)

A review of the user profile data on the laptop also showed that on March 19, 2008, at 10:59 am, a user profile was created on the laptop computer for CG's partner-in-charge, [REDACTED]. This user profile ([REDACTED] 2549) was used on March 21, 2008, to log on to the computer and access saved training files, including a slide show presentation related to federal sector audits. This information suggested that [REDACTED] used the laptop on or around March 21st to give a training presentation. [REDACTED] use of the CG laptop from the network equipment room was never recorded on CG's equipment check out log.

In addition, the OIG's review of the hard drive's user profile data found no activity on the CG laptop from April 2008 through February 2009. Also, a review of CG's equipment check out log also showed no check out entries for the laptop during this period. On September 26, 2008, [REDACTED] conducted a routine physical inventory inspection of the network equipment room in the Calverton office. During this September 26th inspection, [REDACTED] verified that the CG laptop was being stored in the secure network equipment room in the Calverton office.

On February 2, 2009, CG's executive assistant [REDACTED] removed the CG laptop from the network equipment room for use by CG senior auditor [REDACTED].

██████████ walked the laptop up to ██████████, administrative assistant, who recorded its serial number (2UA508087J) on an equipment check out log ██████████ made ██████████ sign an equipment check out form when she took the laptop.

Once ██████████ received the laptop from ██████████, she contacted ██████████ to gain access to the laptop. ██████████ instructed ██████████ over the telephone on how to set up user profile identifications (ID) for the FX Engagement program and the Windows operating system (“0026Temp”). On the following day, February 3rd, ██████████ delivered the laptop computer to Roy CONNOR at the FCC in Washington, DC. (Attachment 9)

CG concluded that it retained custody of the laptop during the four month period between October 2008 and January 2009. This conclusion was supported by the fact that ██████████ verified the physical presence of the laptop in the network equipment room on September 26, 2008; no further user profile activity was identified on the hard drive during this period; and ██████████ retrieved the laptop from the network equipment room on February 2, 2009. No incidents of theft or misuse were reported by CG during this period. (Attachment 9) The laptop has remained in FCC OIG custody pending the completion of the OIG’s investigation.

E. Why was FEC data released to the FCC/OIG?

Answer Summary: CG provided the FCC with a laptop to view electronic audit workpapers. The FCC was unable to view the documents because the original laptop was missing a required software program. In the urgency to provide the FCC with the correct software program, CG partners decided to provide the FCC OIG with a temporary “loaner” laptop until the correct program could be installed on the original laptop given to the FCC.

The CG laptop containing FEC data was randomly selected from the computer network room for use by the FCC. Before the CG laptop was given to the FCC, CG auditor ██████████ prepared it for transfer to the FCC OIG. ██████████ manually removed data on the laptop that was stored in the recycle bin and the FX engagement program. ██████████ was unaware of the FEC data stored on the laptop because it was saved in a renamed folder on the C: drive. Due to the urgency of the FCC OIG request, CG did not reformat the laptop before transferring it to the FCC.

FCC OIG Audit Director Roy Connor discovered the FEC data on the laptop on Thursday, February 5, 2009. Roy Connor reported it to CG on Friday, February 6, 2009, at 3:50 pm. At 4:30 pm, on Friday, February 6th, Roy Connor told CG IT partner, ██████████ that he discovered FEC data on the laptop. CG never notified the FEC of the unauthorized disclosure. The FEC OIG contacted CG regarding the disclosures on February 10, 2009. CG’s partner ██████████ said he didn’t notify the FEC of the data release because Roy Connor did not provide enough information about the incident and

██████████ wanted to better understand the situation. CG's partner ██████████ reported that CG did file an internal incident report to document the release on Saturday, February 7th.

The network computer room in CG's Calverton office stored two types of "loaner pool" laptops. The first loaner type was spare laptops for in-house use by CG employees only. The second type of spare laptops in the "loaner" pool was those designated for client or subcontractor use. (Attachment 9) ██████████ or ██████████ configured these laptops for client use with the FX Engagement installation. Once a laptop was configured, ██████████ placed a label or sticky on it to show which client or subcontractor it was intended for.

The laptops in the network room were either waiting to be taken to a client or were returned to CG by a client. Once a laptop was returned by an auditor after use, it was given to ██████████ or some other administrative staff, who was supposed to note its return on the equipment log and then secure it in the network room. (Attachment 9) ██████████ would come to the Calverton office and clean the client data from the laptop after use; and then he would leave it in the network room for future use. ██████████ placed a label marked "spare" on the returned laptops that he cleaned.

On February 2, 2009, when ██████████ retrieved a laptop from the network room for ██████████ to give to the FCC, she found no laptops in the room that were labeled as a "spare." ██████████ randomly selected the CG laptop without any knowledge of the data it contained. The CG laptop was labeled with a post-it note that read substantially "EBann." ██████████ had to check and make sure the laptop wasn't reserved for someone else.

██████████ was interviewed regarding the circumstances surrounding why she gave the CG laptop that contained FEC data to the FCC. She advised:

She was an IT auditor assigned to work on FCC audits for the last three years. On Monday, February 2nd, Roy CONNOR, of the FCC OIG, informed her that he was unable to view audit workpapers on the laptop computer CG provided him. The laptop was missing a program installation known as Audit Program Generator (APG). ██████████ discussed the matter with CG partners ██████████ and ██████████ and they decided to provide CONNOR a temporary laptop from the network equipment room that already contained the APG software installed.

██████████ contacted CG's system administrator ██████████ for access to the computer. ██████████ provided her a password for the operating system over the telephone. When ██████████ gained access to the laptop, she never saw FEC data on the computer and never knew any data was saved to it. She did not review directories in the computer beyond the computer desktop. She was unaware that files containing FEC data were on the laptop.

CONNOR was interviewed regarding the circumstances surrounding his discovery of the FEC data on the CG laptop. He advised:

In 2008, CG performed an annual audit of the FCC, as required under the Federal Information Security Management Act of 2002 (FISMA). CONNOR had oversight responsibility for the audit. CG provided CONNOR a laptop containing electronic audit workpapers for him to review. CG used a software program called FX Engagement to store its workpapers on both the server and laptops. CONNOR saw a folder on the CG laptop called "FX Engagement.old" in the Windows Explorer directory. This folder contained approximately 400 files, which appeared to be workpapers related to an FEC information technology (IT) audit that ended in September 2007. It was clear from the data that CG never cleaned this laptop after the FEC audit. He observed FEC system security plans. For example, on page 13 of a document entitled "IT Planning Memo," which was dated September 30, 2007, he saw a network diagram of the FEC's internal computer system. This data would not be considered public information.

Connor discovered the FEC data on the laptop on Thursday, February 5, 2009. The next day, Friday, February 6, 2009, at 3:50 pm, he reported the incident to CG auditor [REDACTED]. That same Friday, at 4:30 pm, he received a call from CG partner [REDACTED]. During this telephone conversation, CONNOR informed [REDACTED] that he discovered FEC audit data on the laptop CG provided to him. [REDACTED] told CONNOR that [REDACTED] now had the original laptop meant for the FCC, with the correct program now installed. [REDACTED] said he wanted to switch the laptops out and get back the laptop with the FEC data on it.

On Monday, February 9, 2009, [REDACTED] called CONNOR to schedule a time to come out to the FCC and switch out the laptops. CONNOR said he would be available on Tuesday, February 10th. The next day, February 10th, [REDACTED] and [REDACTED] came out to give CONNOR the new laptop. That same day, the FEC IT security officer and the FEC OIG Deputy IG came to the FCC to review the data files.

CG's senior auditor [REDACTED] investigated the incident to determine why the FEC data was released to the FCC. In the CG report, [REDACTED] wrote:

In September 2008, CG provided the FCC OIG a laptop, which was missing the APG software program that the FCC OIG needed to view electronic workpapers. On January 28, 2009, CG received a "seemingly harsh" email from the FCC OIG that was "strong in its tone," and heightened tensions between CG and the FCC.⁵ On February 2, 2009, CG

⁵ INVESTIGATOR'S NOTE: The issue between CG and the FCC OIG arose because the FCC OIG was unable to view electronic audit workpapers on a different laptop that CG provided to the FCC OIG in September 2008. This first laptop was missing a software program ("APG") that was needed to view the audit documents.

partners [REDACTED] and [REDACTED] decided to provide the FCC OIG a replacement machine, rather than taking the time to pick up the laptop and have Service Operations fix/repair it. [REDACTED] and [REDACTED] directed [REDACTED]... to pull a loaner machine from the secure storage room. (Attachment 9, page 13)

In the CG report, [REDACTED] reported the results of his interview with [REDACTED]
[REDACTED] According to [REDACTED], [REDACTED] advised:

In order to do something quickly [to resolve the FCC OIG issue], the decision was made by those partners [REDACTED] and [REDACTED] to switch out the laptop with a “loaner” machine that may be available. She [REDACTED] then coordinated with an administrative person in the Calverton office to pull a “temp” laptop out of the locked storage... The laptop pulled was labeled with “EBAN” on it... She then also coordinated over the phone to delete items in the “Recycle Bin” and also to delete all other FX binders through FX Engagement. (Attachment 9, pages 15 and 16)

[REDACTED] was questioned as to why the CG laptop was given to the FCC without first being reformatted. He was also questioned as to why he did not report the disclosure incident to the FEC OIG. In response to these questions, [REDACTED] advised:

[REDACTED] felt an urgency to quickly give the FCC a replacement computer when he learned the original computer provided to the FCC was not working, because CG had provided the FCC OIG with audit workpapers, for review, back in August 2008. Then six months later, in February 2009, [REDACTED] learned that the FCC audit workpapers had not yet been reviewed by the FCC OIG. [REDACTED] wanted this FCC OIG review of the audit workpapers to occur as quickly as possible, so that the audit could have some finality. [REDACTED] had no knowledge that the replacement laptop still contained FEC data on it, when the laptop was furnished to the FCC.

[REDACTED] did not notify the FEC of the data release because Roy Connor did not provide him with enough information about the incident. CONNOR was being evasive about how he found the FEC data and what kind of data he found. [REDACTED] wanted to better understand the situation and the see what data was released before reporting the incident.

CG partner [REDACTED] advised that CG filed an internal incident report to document the release on that Saturday, February 7th.

F. What data encryption and password controls did CG use to protect FEC data?

Answer Summary: CG did not install Pointsec encryption software on the CG laptop in question until March 8, 2008, at 10:32 am. This encryption installation occurred four months after the completion of the 2007 FEC audit and six months after CG's partner [REDACTED] agreed to install the encryption software.

CG staff reportedly wrote user names and passwords on laptops, in connection with Federal audits, on three or four occasions. First, CG placed a post-it note with a user name and password on the CG laptop assigned to [REDACTED]. Second, CG auditor [REDACTED] placed a post-it note with a user name on the CG laptop assigned to Roy Connor. [REDACTED] later wrote the password on the post-it note when she gave the laptop to Connor. And finally, FCC OIG employee Roy Connor reported that CG staff placed a user name and password on post-it notes attached to laptops that were given to two other FCC OIG employees, Sophie Jones and Sharon Spencer.

On September 5, 2007, [REDACTED], CG's IT partner, sent a letter to Alec PALMER, the FEC CIO, in which he agreed that CG would encrypt all FEC data on all Clifton Gunderson laptops. [REDACTED] gave this assurance, among others, so the FEC would waive the FEC Mobile Computing Security Policy (Policy Number 58-4.3) that all laptops accessing the FEC network must be encrypted and have a two-factor authentication mechanism. (Attachment 7) Although CG was deploying encryption software on some CG laptops in 2007 and 2008, the technology did not meet the specific requirements contained in the FEC policy.

CG's senior auditor [REDACTED] investigated this agreement to determine if CG honored this promise to provide encryption protections. On page 6 of the CG report, [REDACTED] wrote:

“The encryption utility is PointSec version 6.2.0. PointSec is a required loadset... and was installed on all machines during the middle of 2007. The authentication method for PointSec is a “pass through” authentication of the Windows logon... therefore, two-factor authentication is not used. (Attachment 9)

During the OIG investigation, a review of a copy of the CG laptop's hard drive was conducted at the FCC. Also present during this review were Roy CONNOR, and CG employees, [REDACTED] and [REDACTED]. Despite the claim made in [REDACTED] report, the OIG review determined that CG's End User Support staff installed the encryption software PointSec on the CG laptop on March 8, 2008, at 10:32am. (Attachment 10) [REDACTED] did not report this observation in the CG report. During an interview, CG partners [REDACTED] and [REDACTED] claimed that encryption software was installed on laptops used for the FEC audit in 2007; however, neither [REDACTED] nor [REDACTED] were able to provide specific details or any evidence, which supported this claim.

██████████, IT auditor, was interviewed by the OIG regarding encryption software on the Samlin issued laptop he used to perform work on the FY 2007 FEC audit. ██████████ advised that his Samlin laptop now has PGP encryption software installed on it; but he does not recall if the encryption software was installed when he worked on the FEC audit in 2007.

The OIG investigated CG's use of password controls to protect FEC data. This review determined that CG created account usernames and passwords for users to access the FX Engagement program. CG also used user names and passwords to access the Windows operating system on its computers. (Attachment 9, pages 5-6)

██████████ was interviewed regarding how CG provided him with a user name and password for the CG issued laptop. In response to questions, he advised:

In or around July 2007, ██████████ delivered the CG laptop to ██████████ at the FEC for his use. The CG laptop was password protected. ██████████ provided him with a user name and password to logon to the computer, and another user name and password to access the local copy of FX engagement. The user names and passwords for the CG laptop were provided to ██████████ on a yellow post-it that was taped to the laptop. He recalled that one of his user names was "EBANN." He did not know if it was ██████████ or someone in CG's IT department who placed the post-it note on the laptop. He kept the post-it in his wallet until he memorized the user names and passwords; then he kept the post it in a locked cabinet in his home.

In August 2007, when he was completing his portion of the audit, ██████████ returned the CG laptop to ██████████. This occurred at the FEC. ██████████ initially said he placed the original yellow post-it note back on the CG laptop when he returned it to ██████████. In a subsequent interview, ██████████ said he did not put the post-it note back on the laptop when he returned it to ██████████.

CONNOR, FCC OIG IT Director, was interviewed regarding how CG provided him with a user name and password for the CG laptop that was found to contain FEC data. He advised that in February 2009, when CG auditor ██████████ gave him the laptop, the user name and password to access the laptop was on a post-it note that was attached to the laptop.

██████████ CG senior IT auditor on the FCC contract, was interviewed regarding how she provided CONNOR with the user name and password for the CG laptop. In response to questions, she advised:

She signed the laptop out of the network room on Monday, February 2nd, and delivered it to CONNOR on Tuesday, February 3rd. When she received this laptop, it had a post-it note on it that said something like "EBann." She threw this old post-it note away and

replaced it with a new post it that said user ID “0026Temp,” which was the user profile that [REDACTED] helped her create that same day by telephone.

When [REDACTED] replaced the old post-it note on the laptop, she wrote the user id for the operating system (00026Temp) and the user id and password for FX Engagement on a new post-it note. [REDACTED] also provided her with the password to the operating system over the telephone. [REDACTED] did not write the operating system password on the post-it note until she arrived in [REDACTED]’s office. She had memorized this password in her head. When she delivered the laptop to the FCC, she asked [REDACTED] if he wanted her to write down the operating system password on the post it note. [REDACTED] nodded his head as if to indicate yes. Based on [REDACTED]’s nod, [REDACTED] wrote down the password while she was in [REDACTED]’s office.

CG’s senior auditor [REDACTED] investigated the password incident at the request of the FEC OIG. The CG report contradicted [REDACTED] and [REDACTED]’s statements during the OIG interviews. According to [REDACTED], it was [REDACTED] who made the request to [REDACTED] to write down the password to the operating system on the post-it note. On page 5 of the CG report, [REDACTED] wrote:

The account and password to the FX application were written down, as was the userID for the laptop (Windows). However, the password to Windows was written down per the request of the FCC OIG representative... The FCC OIG contact indicated that “may have been” the circumstances – but that he didn’t really recall what had transpired... [REDACTED] believes this is how it happened, but wasn’t sure whether there was a specific request to write down the Windows password,⁶ or the precise circumstances – but that she knew it was written down in front of the FCC OIG contact, and that she believed he requested that she write this down for him. (Attachment 9)

In the Summary of Observations section of the CG report, on page 11, observation #3, [REDACTED] again concluded, without support, that “[i]t is likely and reasonable that FCC OIG requested that the windows account password be also written on the laptop. Then on page 13 of the CG report, [REDACTED] again appeared to contradict his previous assertions by stating:

During the meeting when she [REDACTED] delivers the machine, there is a collective decision (it is not clearly recalled by either whether the FCC OIG asked for this to be done specifically – but both agree it was written down with both of them in

⁶ The CG report contradicted its own account of the password events by first stating that CONNOR requested the password to be written down, and then it stated that [REDACTED] wasn’t sure whether a specific request was made.

acknowledgment and present) to also write down the windows password onto the laptop as well.⁷ (Attachment 9)

In the “Summary of Interviews Conducted” section of the CG report, near the bottom of page 17, [REDACTED] stated:

She [REDACTED] acknowledged that it wasn’t good judgment to put the FX account and password onto the laptop. However, it is her assertion that the only reason she put the password to the windows domain account was that the FCC OIG asked her what the new password was, and that he indicated it was OK for her to go ahead and write this on the note taped to the laptop as well. This information was then only documented along with the laptop at the consideration and in the presence of the FCC OIG contact.⁸ (Attachment 9)

During the OIG’s interview of Roy CONNOR, he was advised of [REDACTED] recollection of the events, concerning how the password ended up being written on the post it note. In response to questions, CONNOR advised:

He did not recall [REDACTED] writing the password on the post-it note in front of him while she was in his office. He cannot say for certain that she didn’t write the password down in front of him. He did not recall one way or the other. It did appear, however, that the user name and the password were written at different times. The user name was written in black ink and the password was written with blue ink. He did not recall that [REDACTED] asked him if he wanted her to write down the password on the post it. That would be a security taboo to write down a password on the laptop.

CONNOR’s coworkers at the FCC-OIG have received laptops from CG in the past with user names and passwords written on the laptops. For example, FCC employee Sophie Jones received a laptop from CG that had a “sticky” on the back with the user name and password written down. On Jones’ laptop, the user name and password were not labeled as “user name” and “password.” FCC employee Sharon Spencer also received a laptop from CG with the user name and password written on a yellow post-it not, attached to the laptop.

⁷ [REDACTED] assertion on page 13 that Roy CONNOR acknowledged [REDACTED] writing down the password in his presence conflicts with CONNOR statement to the OIG, that he had no recollection of [REDACTED] writing the password down in front of him.

⁸ [REDACTED] provided an interview statement to the OIG that was consistent with this account of the events.

V. FINDINGS

During the course of this investigation, the OIG found reasonable cause to believe that CG did not comply with FEC's data security requirements. These findings included:

- CG disclosed sensitive FEC information to the FCC OIG without authorization. Although this unauthorized disclosure was apparently accidental, and it was limited only to the FCC OIG, it did not comply with the FEC non-disclosure agreements.
- CG failed to take reasonable precautions to protect FEC data against the unauthorized disclosure. The laptop was not reformatted or reimaged prior to transfer to a new client.
- CG failed to remove sensitive FEC data from its laptop, as agreed, within 90 days of the conclusion of the audit. The audit concluded on November 13, 2007. The FEC data remained on the laptop long after the 90 day deadline of February 2008. This violated Commission Directive 58, which required CG to erase all sensitive FEC data from its laptops.
- CG failed to encrypt FEC data on its laptop within a timely manner. The encryption software "Pointsec" was not installed on the CG laptop until March 8, 2008. This omission did not comply with the FEC Mobile Computing Security Policy, Number 58-4.3. This omission also did not comply with the assurance that CG gave to the CIO, in a letter dated September 5, 2007.
- CG failed to immediately report to the FEC the unauthorized disclosure of FEC data. CG partner [REDACTED] learned of the data release on Friday, February 6, 2009, at 4:30pm. [REDACTED] failed to call the FEC to report the incident, on that Friday, or on the following Monday. This conduct did not comply with the FEC non-disclosure agreements.

VI. RECOMMENDATIONS

During the course of the investigation, a number of data security vulnerabilities involving contractors were found, which warrant improvement. The OIG has identified three issues and this report provides suggestions for improvement. The current status of the issues is also discussed.

Based upon the results of this investigation, the OIG makes the following recommendations to improve the protection of sensitive FEC data:

Suggestion 1: The FEC should incorporate contractor data security standards in all FEC contracts. The placement of these standards as a contract requirement will emphasize their importance.

Status: The OIG implemented a policy entitled “FEC OIG Contractor Security Standards” to strengthen data security controls on all future OIG audit contracts. This policy has been presented to the FEC CIO for consideration on all FEC contracts. (Attachment 11)

Further, the FEC CIO and ISSO drafted new “Minimum Contractor System Security Standards,” to be incorporated in future FEC contracts. The OIG has already incorporated the new contract language prepared by the CIO and ISSO into the OIG’s new financial statement audit contract signed in April 2009 (Exhibit D – FEC Clauses & Special Provisions). (Attachment 12)

Suggestion 2: The FEC should require contractors and FEC COTR personnel to make post contract inspections and certifications to ensure that FEC data is removed from laptop computers.

Status: The OIG has preliminarily discussed the need for post contract follow ups with the CIO and ISSO.

Suggestion 3: The FEC should improve its identification of data that is, or should be, classified as “sensitive.” This identification process should be similar to the process undertaken by the FEC to identify personally identifiable information (PII).

Status: The OIG has preliminarily discussed with the CIO and ISSO the need to identify and mark sensitive FEC data. This need has even greater importance when the sensitive information is being provided to contractors.

VII. PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE

This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENTS

Attachments #	Description
1	FEC contract FE-4-AC-0065, awarded to Clifton Gunderson LLP for audit services, including the Statement of Work (SOW)
2	Completion of mandatory FEC security awareness training, signed in May and June of 2007, by Clifton Gunderson partners and employees
3	FEC Commission Directive No. 58, effective January 16, 2007
4	FEC Mobile Computing Security Policy No. 58-4.3
5	FEC Non-Disclosure Agreement, signed in 2007 by Clifton Gunderson partners and employees
6	FEC Nondisclosure Agreement for Contractors, signed in 2008 by Clifton Gunderson partners and employees
7	Letter from [REDACTED] to Alec Palmer, dated 09/05/07
8	CG documents provided by [REDACTED] on 02/12/09: Wireless Equipment Checkout (Ticket #1083), dated 02/02/09; Wireless Equipment Checkout (Log)
9	Clifton Gunderson Report on FEC Data Concern, dated 06/02/09
10	Fax from Roy Connor, FCC OIG, showing log screen shot for Pointsec installation
11	FEC OIG Contractor Security Standards
12	Minimum Contractor System Security Standards, prepared by the CIO and ISSO, incorporated into the FEC OIG Financial Audit Exhibit D – “FEC Clauses & Special Provisions”

Attachment No. 1

FEC contract FE-4-AC-0065, awarded to Clifton Gunderson LLP
for audit services, including the Statement of Work (SOW)

Case Number INV-09-02

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

Offeror to Complete Blocks 12, 17, 23, 24, & 30

1. Requisition Number: FECC10-04-6138
PAGE 1 OF 8

Contract No. 03F0135L
3. Award/Effective Date: Feb. 25, 2004
4. Order Number: FE1AC0065
5. Solicitation Number: FE1AC0065
6. Solicitation Issue Date: /
7. Telephone Number (No collect calls): 202-594-1328
8. Offer Due Date/Local Time: /

Issued By: FEDERAL ELECTION COMMISSION
9 E STREET NW
ATTN: JACQUELYN CONNELL
WASHINGTON, DC 20463
Code: ADMIN6
10. This Acquisition is:
 Unrestricted
 Set-Aside % for:
 Small Business
 HubZone Small Business
11. Delivery for FOB Destination Unless Block is Marked:
 See Schedule
12. Discount Terms:
Discount: 0%
Net Due: 30
13a. This contract is a rated order under DPAS (15 CFR 700)

13b. Rating:
14. Method of Solicitation:
 RFQ IFB RFP

Deliver To: SCHEDULE
Code: 00001
16. Administered By: FEDERAL ELECTION COMMISSION
999 E STREET NW
ATTN: JACQUELYN CONNELL
WASHINGTON, DC 20463
Code: ADMIN6

a. Contractor/Offeror: JEFFON GUNDERSON LLP
11 Powder Mill Road, Suite 410
Iverson MD 20705
Code: 00001154 Facility Code:
Telephone No. 301-931-2050 TIN: 370802863
17a. Payment Will Be Made By: FEDERAL ELECTION COMMISSION
ATTN: FINANCE OFFICE RM 620A
999 "E" ST., NW
WASHINGTON, DC 20463
Code: ACCOUNT

b. Check if Relationship is Different and Put Such Address in Offer:

18. Submit Invoices to Address Shown in Block 17a Unless Box Below is Checked:
 See Addendum.

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Fixed Price Order under GSA Schedule GS-23F-0135L- Terms and Conditions under the schedule				

Accounting and Appropriation Data: 11600.85. BOC: 2521
26. Total Award Amount (For Govt. Use Only): US 76,106.00

27a. Solicitation incorporates by reference FAR 52.212-1, 52.212-4, FAR 52.212-3 and 52.212-5 are attached. Addenda are are not attached
27b. Contract/Purchase Order incorporates by reference FAR 52.212-4, 52.212-5 is attached. Addenda are are not attached

28. Contractor is required to sign this document and return copies to Issuing Office. Contractor agrees to furnish and deliver all items set forth or otherwise identified above and on any additional sheets subject to the terms and conditions specified herein.
29. Award of Contract Reference: Quote dated Jan 5, 2004 Offer Dated: / Your offer on Solicitation (Block 5), including any additions or changes which are set forth herein, is accepted as to items:

30. Signature of Offeror/Contractor: *Patrick M. Byer, Sr.*
31a. United States of America (Signature of Contracting Officer): *Jacquelyn Connell*
31b. Name of Contracting Officer (Type or Print): Jacquelyn Connell
31c. Date Signed: 2/25/2004
30c. Date Signed: 2/24/04
31c. Date Signed: 2/25/2004

Quantity in Column 21 Has Been:
 Received Inspected Accepted and Confirms to the Contract, Except as Noted:

Signature of Authorized Government Representative: /
32c. Date: /
32d. Printed Name and Title of Authorized Government Representative:
32f. Telephone Number of Author Govt Government Representative:
32g. E-mail of Authorized Government Representative:

34. Voucher Number: /
35. Amount Verified Correct For: /
36. Payment: Complete Partial Final
37. Check Number:
38. S/R Voucher Number: /
40. Paid By: /

I certify this account is correct and proper for payment
Signature and Title of Certifying Officer: /
41c. Date: /
42a. Received By (Print): /
42b. Received At (Location): /
42c. Date Rec'd (YY/MM/DD): /
42d. Total Contract Amount: 76,106.00
42d. Total Contract Amount: 76,106.00

SCHEDULE Continued

Item No.	Supplies/Services	Quantity	Unit	Unit Price	Amount
	contract apply to this order				
	Point of contact at Federal Election Commission for contract coordination and invoice certification: Jon Hatfield, 202-694-1018				
	Contractor shall provide Audit Services to the Office of Inspector General for the Federal Election Commission				
	BASE YEAR- FEBRUARY 23, 2004 THROUGH DECEMBER 30, 2004				
1	Audit of the FEC Financial Statements in accordance to the SOW.	1	LT	76,106.00	76,106.00
	OPTION YEAR ONE - JANUARY 1, 2005 THROUGH DECEMBER 31, 2005				
2	Audit of FEC Financial Statement in accordance to SOW	1	LT	74,336.00	74,336.00
	OPTION PERIOD TWO - JANUARY 1, 2006 THROUGH DECEMBER 31, 2006				
3	Audit of FEC Financial Statement in accordance to SOW	1	LT	76,552.00	76,552.00
	OPTION PERIOD THREE - JANUARY 1, 2007 THROUGH DECEMBER 31, 2007				
4	Audit of Financial Statements in accordance to the SOW	1	LT	78,962.00	78,962.00
	OPTION PERIOD FOUR - JANUARY 1, 2008 THROUGH DECEMBER 31, 2008				
5	Audit of FEC Financial Statement in accordance to SOW	1	LT	81,178.00	81,178.00
6	DELIVERABLES- to be provided in accordance to the SOW are not priced separately from the total costs.	1	LT	NSP	NSP

Table of Contents

Page

SECTION B 4

B.1 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (Oct 2003)..... 4

B.2 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR
EXECUTIVE ORDERS--COMMERCIAL ITEMS (JAN 2004)..... 4

B.3 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)..... 6

B.4 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)..... 6

B.5 ADDENDA Z:\GauditSOWfinal.rtf..... 7

SECTION B

B.1 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (Oct 2003)
(Reference 12.301)

B.2 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR
EXECUTIVE ORDERS--COMMERCIAL ITEMS (JAN 2004)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clause, which is incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items: 52.233-3, Protest after Award (AUG 1996) (31 U.S.C. 3553).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: [Contracting Officer check as appropriate.]

XX (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (JUL 1995), with Alternate I (OCT 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

_____ (2) 52.219-3, Notice of Total HUBZone Set-Aside (JAN 1999) (15 U.S.C. 657a).

_____ (3) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 1999) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

_____ (4) (i) 52.219-5, Very Small Business Set-Aside (JUNE 2003) (Pub. L. 103-403, section 304, Small Business Reauthorization and Amendments Act of 1994).

_____ (ii) Alternate I (MAR 1999) of 52.219-5.

_____ (iii) Alternate II (JUNE 2003) of 52.219-5.

_____ (5) (i) 52.219-6, Notice of Total Small Business Set-Aside (JUNE 2003) (15 U.S.C. 644).

_____ (ii) Alternate I (OCT 1995) of 52.219-6.

_____ (6) (i) 52.219-7, Notice of Partial Small Business Set-Aside (JUNE 2003) (15 U.S.C. 644).

_____ (ii) Alternate I (OCT 1995) of 52.219-7.

_____ (7) 52.219-8, Utilization of Small Business Concerns (OCT 2000) (15 U.S.C. 637 (d) (2) and (3)).

_____ (8) (i) 52.219-9, Small Business Subcontracting Plan (JAN 2002) (15 U.S.C. 637(d) (4)).

_____ (ii) Alternate I (OCT 2001) of 52.219-9.

_____ (iii) Alternate II (OCT 2001) of 52.219-9.

_____ (9) 52.219-14, Limitations on Subcontracting (DEC 1996) (15 U.S.C. 637(a) (14)).

_____ (10) (i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (JUNE 2003) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

_____ (ii) Alternate I (JUNE 2003) of 52.219-23.

_____ (11) 52.219-25, Small Disadvantaged Business Participation Program-Disadvantaged Status and Reporting (OCT 1999) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

_____ (12) 52.219-26, Small Disadvantaged Business Participation Program-Incentive Subcontracting (OCT 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

XX (13) 52.222-3, Convict Labor (JUNE 2003) (E.O. 11755).

_____ (14) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2004) (E.O. 13126).

XX (15) 52.222-21, Prohibition of Segregated Facilities (FEB 1999).

XX (16) 52.222-26, Equal Opportunity (APR 2002) (E.O. 11246).

XX (17) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (DEC 2001) (38 U.S.C. 4212).

SECTION B

XX (18) 52.222-36, Affirmative Action for Workers with Disabilities (JUN 1998) (29 U.S.C. 793).

XX (19) 52.222-37, Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (DEC 2001) (38 U.S.C. 4212).

_____ (20) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA Designated Products (AUG 2000) (42 U.S.C. 6962(c)(3)(A)(ii)).

_____ (ii) Alternate I (AUG 2000) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)).

XX (21) 52.225-1, Buy American Act-Supplies (JUNE 2003) (41 U.S.C. 10a-10d).

_____ (22) (i) 52.225-3, Buy American Act-Free Trade Agreements- Israeli Trade Act (Jan 2004) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, Pub. L. 108-77, 108-78).

_____ (ii) Alternate I (Jan 2004) of 52.225-3.

_____ (iii) Alternate II (Jan 2004) of 52.225-3.

_____ (23) 52.225-5, Trade Agreements (Jan 2004) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

XX (24) 52.225-13, Restrictions on Certain Foreign Purchases (OCT 2003) (E.o.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

_____ (25) 52.225-15, Sanctioned European Union Country End Products (FEB 2000) (E.O. 12849).

_____ (26) 52.225-16, Sanctioned European Union Country Services (FEB 2000) (E.O. 12849).

_____ (27) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

_____ (28) 52.232-30, Installment Payments for Commercial Items (OCT 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

XX (29) 52.232-33, Payment by Electronic Funds Transfer-Central Contractor Registration (OCT 2003) (31 U.S.C. 3332).

_____ (30) 52.232-34, Payment by Electronic Funds Transfer-Other than Central Contractor Registration (MAY 1999) (31 U.S.C. 3332).

_____ (31) 52.232-36, Payment by Third Party (MAY 1999) (31 U.S.C. 3332).

XX (32) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

_____ (33) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (APR 2003) (46 U.S.C. Appx 1241 and 10 U.S.C. 2631).

_____ (ii) Alternate I (APR 1984) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: [Contracting Officer check as appropriate.]

_____ (1) 52.222-41, Service Contract Act of 1965, as Amended (MAY 1989) (41 U.S.C. 351, et seq.).

_____ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

_____ (3) 52.222-43, Fair Labor Standards Act and Service Contract Act-Price Adjustment (Multiple Year and Option Contracts) (MAY 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

_____ (4) 52.222-44, Fair Labor Standards Act and Service Contract Act-Price Adjustment (February 2002) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

_____ (5) 52.222-47, SCA Minimum Wages and Fringe Benefits Applicable to Successor Contract Pursuant to Pre-December 1993 Contractor Collective Bargaining Agreements (CBA) (May 1989) (41 U.S.C. 351, et seq.).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vi) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.219-8, Utilization of Small Business Concerns (October 2000) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$500,000 (\$1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (April 2002) (E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (December 2001) (38 U.S.C. 4212).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998) (29 U.S.C. 793).

(v) 52.222-41, Service Contract Act of 1965, as Amended (May 1989), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, et seq.).

(vi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (April 2003) (46 U.S.C. Appx 1241 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor May include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

B.3 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within Sixty (60) days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least Sixty (60) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of clause)

B.4 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond _____ The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond _____ until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

B.5 ADDENDA

STATEMENT OF WORK For Audit Services Federal Election Commission

1. INTRODUCTION

The Federal Election Commission (FEC) is an independent Federal agency established by the Congress as a Commission. The FEC is responsible for administering and enforcement of the Federal Election Campaign Act (FECA). The FEC administers and enforces the FECA through the four core programs of disclosure, compliance, Presidential public funding, and election administration.

Disclosure involves receiving reports of campaign finance transactions by candidates and political committees involved in elections for Federal office and promulgating them as part of the public record.

Compliance involves the review and assessment of campaign finance transactions to ensure that filers abide by the appropriate limitations, prohibitions, and disclosure requirements of the FECA. Compliance also involves oversight of individual contributors, corporations, labor unions, and "issue" groups that, although they may not fit within the universe of filers, can be involved in violations of the FECA. The FEC has exclusive jurisdiction over civil enforcement of the FECA and engages in civil enforcement proceedings to resolve instances of noncompliance.

Presidential public funding is the system for financing Presidential primaries, general elections, and national party conventions. Congress designed the program to correct the campaign finance abuses perceived in the 1972 Presidential electoral process. Congress designed a program that combines public funding with limitations on contributions and expenditures. The program has three parts: (1) Matching funds for primary candidates; (2) funds to sponsor political parties' Presidential nominating conventions; and (3) funds for the general election campaigns of major party nominees and partial funding for qualified minor and new party candidates. Based on statutory criteria, the Commission determines which candidates and committees are eligible for public funds, and in what amounts. The U.S. Treasury then makes the necessary payments. Later the FEC audits all the committees that received public funds to ensure that they used the funds in accordance with the FECA, public funding statutes, and FEC regulations. Based on the Commission's audit findings, Presidential committees may have to make repayments to the U.S. Treasury.

The Office of Election Administration serves as a central exchange for the compilation and dissemination of information and research on issues related to the administration of Federal elections. This office issued voluntary performance and test standards that states and voting systems

vendors can use to improve the accuracy, integrity, and reliability of computer-based systems. The Office also helped states implement the National Voter Registration Act (NVRA) of 1993, which Congress enacted to facilitate and increase voter registration by providing opportunities to register at a number of state agencies, using a number of registration methods. The Help America Vote Act of 2002 calls for the functions of the FEC's Office of Election Administration to be transferred to a new commission called the Election Assistance Commission.

The FEC is headed by six commissioners, appointed by the President and confirmed by the Senate. Commissioners serve a six year term and no more than three Commissioners may represent the same political party. By statute, the Commissioner chairmanship rotates every year, and the designated chairman has limited authority to set the agency's agenda.

Under the Commissioners, the FEC's organizational structure is separated into three primary offices: the Office of the Staff Director (OSD), the Office of the General Counsel (OGC), and the Office of Inspector General (OIG), each headed by a statutory officer. Subordinate offices to the General Counsel are titled Associate General Counsels, and each supports one or more of the four core FEC programs. Subordinate organizations to the Staff Director are in most cases called "offices" for staff support activities and "divisions" for line activities that are involved in one or more of the four core programs. Programmatic elements under the Office of the Staff Director include the Disclosure Division, Information Technology, Information Division, the Press Office, Reports Analysis Division (RAD), Audit Division, and the Office of Election Administration. The Office of Inspector General is headed by the Inspector General and reports directly to the Commission.

In FY 2003, the FEC was provided 389 full time equivalents (FTEs) and a budget of \$49,541,871.00, of which approximately 66% was budgeted for staff salaries and benefits, 7% for office space rental, and 27% on all other expenses. The FEC is located in Washington DC and has no regional offices. Additional background on the FEC, including budget submissions, annual performance plans and reports, as well as mission and organizational structure are available at the FEC's website at <http://www.fec.gov/>.

2. BACKGROUND

a. Federal Financial Accounting System

On October 19, 1999 the American Institute of Certified Public Accountants (AICPA) recognized the Federal Accounting Standards Advisory Board (FASAB) as the body designated to establish generally accepted accounting principles (GAAP) for Federal governmental entities under Rule 203, "Accounting Principles," of the AICPA's Code of Professional Conduct. The FEC financial statements are prepared in accordance with GAAP for Federal government entities.

The basis consists of the following hierarchy:

1. Accounting standards and principles recommended by the Federal Accounting Standards Advisory Board (FASAB). These are known as Statements of Federal Financial Accounting Standards (SFFAS) and Statements of Federal Financial Accounting Concepts (SFFAC).
2. Form and content requirements in OMB Bulletin 01-09.
3. Accounting standards contained in FEC's accounting policy manuals and handbooks.

4. Accounting principles published by authoritative standards-setting bodies (e.g., Financial Accounting Standards Board) and other authoritative sources (a) in the absence of other guidance in the first parts of this hierarchy, and/or (b) if the use of such accounting standards improves the meaningfulness of these financial statements.

Transactions are recorded on an accrual accounting basis as well as a budgetary basis. Under the accrual method, revenues are recognized when earned and expenses are recognized when a liability is incurred, without regard to receipt or payment of cash. Budgetary accounting facilitates compliance with legal constraints and controls over the use of Federal funds.

The FEC's core Federal financial system is supported by commercial software called PeopleSoft Financials, to include payables and the general ledger. Contracts, purchase orders, interagency agreements, etc. are developed using a commercial procurement software program called Comprizon.Buy. Obligations resulting from these purchases, as well as purchase and fleet charge card transactions, are then manually obligated and entered in the core financial system.

Asset management is the responsibility of two FEC divisions. Office equipment and personal property are accounted for using a commercial software program called Inte-Great Property Manager (IPM).

The FEC's Payroll and Personnel Offices utilize the U.S. Department of Agriculture's National Finance Center (NFC) to process the agency's payroll and personnel data. An interface between the FEC and NFC enables the FEC Payroll and Personnel Offices to input data which is then processed by the NFC.

The FEC's budget formulation system is composed of a series of Microsoft Excel spreadsheets and Word templates that support the development of the Commission's annual budget requests, with reliance on data from the core financial system. The budget system also uses several legacy systems, including a 1032/COBOL based system to generate the FEC's budget projection report. Budgetary limits are entered manually into the core financial system for budgetary control purposes.

b. Fund Accounting Structure

The FEC's financial activities are accounted for by Federal account symbol. They include the accounts for appropriated funds and other fund groups described below for which the FEC maintains financial records.

General Funds - These funds consist of salaries and expense appropriation accounts used to fund the agency operations and capital expenditures.

Deposit and Suspense Accounts - These funds are maintained to account for receipts awaiting proper classification, or held in escrow, until ownership is established and proper distributions can be made.

Receipt Accounts - The FEC collects civil penalties and other miscellaneous receipts, which are not retained by the FEC. These receipts are deposited directly to a U. S. Treasury receipt account.

3. PROJECT OBJECTIVES

Contractor shall conduct an audit, following Generally Accepted Government Auditing Standards, of the Federal Election Commission's Financial Statements (that are prepared in compliance with OMB Bulletin No. 01-09) for Fiscal Year 2004. A fixed price task order under the GSA schedule is contemplated.

The Government Management and Reform Act of 1994 amended the requirements of the Chief Financial Officers (CFO) Act of 1990 by requiring, among other things, the annual preparation and audit of organization-wide financial statements of 24 executive departments and agencies. The FEC was not among the original 24 departments and agencies covered by the CFO Act. In addition, the Federal Financial Management Improvement Act (FFMIA) of 1996 requires that the report on these audits state whether the agency financial management systems comply substantially with the Federal financial management system requirements, applicable Federal accounting standards, and the U.S. Government Standard General Ledger at the transaction level.

In FY 2002, Congress passed the Accountability of Tax Dollars Act of 2002. The Act requires the FEC, along with numerous other Federal entities, to have its financial statements audited annually. The Office of Management and Budget Director granted the FEC a waiver for the fiscal year 2003 annual audit requirement.

The project objective is to provide sufficient audit effort to render to the Inspector General an opinion on the Federal Election Commission's financial statements for fiscal year 2004 in accordance with generally accepted auditing standards, Government Auditing Standards, and OMB Bulletin 01-02. The six financial statements, along with all corresponding notes and supplementary information to be audited include: (a) Balance Sheet; (b) Statement of Net Cost; (c) Statement of Changes in Net Position; (d) Statement of Budgetary Resources; (e) Statement of Financing; and (f) Statement of Custodial Activity.

The specific objectives of the audit are identified in sections 6 through 10 of OMB Bulletin 01-02.

4. SCOPE

a. Audit Phases/FAM

The audit will be completed to enable the OIG to meet the time frames established by OMB. Whenever OMB deadlines change, it is the responsibility of the IPA to plan the audit accordingly.^{1/} Drafts of all written products shall be submitted to the COTR for review and comment. The contractor shall allow sufficient time for the COTR to review each "draft" deliverable and provide written comments. At a minimum, the Government shall be provided ten (10) days^{2/} to review written documents. Any changes required by the COTR, shall be incorporated by the contractor into a final product. All final products shall be delivered within one (1) week after receiving comments from the COTR. The final audit shall be delivered within one (1) week after receiving comments

¹ To meet OMB deadlines for audited financial statements, the IPA should begin select aspects of the audit before the close of the fiscal year. For example, internal controls and compliance testing should be conducted during the fiscal year for which the opinion will be rendered. During this time, audit steps (transaction testing for payroll, travel, vendor payments and subsequent disbursements) may be performed at the FEC.

² Unless otherwise stated, all references to "days" in this Statement of Work shall be considered to be calendar days. If this causes a deliverable to be submitted on a weekend or Federal holiday, it will be due the next work day.

from the COTR, or three (3) work days prior to the OMB due date, whichever is earlier. The audit will be performed in three phases:

1. Planning Phase - Risk assessment and audit program development.
2. Internal Control Evaluation and Compliance Phase - Review and evaluate the existence and effectiveness of internal controls and compliance with laws and regulations.
3. Substantive Testing and Reporting Phase - All work required to issue an opinion on whether the financial statements and associated notes present fairly the financial position of the FEC for the audited fiscal year. This includes the preparation of a management letter.

5. DELIVERABLES

Contractor shall provide the following:

a. Overall planning document, audit programs cross referenced to the working papers, lead sheets. Within two (2) months after the effective date of award, the contractor shall deliver to the COTR an overall planning document, and internal control audit program, a compliance with laws/regulations audit program, and a substantive audit program for the COTR's review and approval. This plan shall establish dates, using the timeframes established for the deliverables identified in this section and the "Audit Phases" section above. Within one (1) week after receipt of comments from the COTR, the contractor shall submit a final document, which incorporates all comments from the COTR. The delivery of a final plan shall be considered a requirement of this task order, and the contractor shall not begin working on any other part of this project until the final plan is approved by the COTR. Should any options be exercised under this task order, the contractor shall submit an updated plan within one (1) month after each option is exercised. The contractor shall incorporate all comments of the COTR into each updated plan within one (1) week after receipt of the comments.

- * The overall planning document identifies the approach and time schedule for the audit, including milestones and due dates (planning, internal control and compliance testing, substantive testing, and reporting).
- * The internal control audit program includes sections on significant internal controls identified during the planning phase, and the nature and extent of tests to be performed.
- * The compliance audit program will identify, at a minimum, all significant laws and regulations that will be covered in the audit, and compliance testing procedures.
- * The substantive audit program includes individual account balances to be tested and the substantive testing procedures to be applied, including the number of transactions to be tested.

b. Report on the internal controls and compliance with laws and regulations - The report will present the results of the internal control evaluation and compliance tests. Any weaknesses that are not reportable conditions should be written up and attached to the draft for later inclusion in the management letter. The contractor shall provide a preliminary draft for review and comment before finalized.

c. Opinion letter - As the principal auditor (see AICPA's Professional Standards, volume 1, AU section 543) the contractor shall sign the opinion letter, which shall be delivered along with the final audit report, and contain the information identified in section 7 of OMB Bulletin 01-02. The contractor shall provide a preliminary draft for review and comment before finalized.

d. Management letter - Within one (1) month after delivery of the final approved audit, the contractor shall deliver a draft management letter in accordance with Section 9 of OMB Bulletin 01-02. All findings are to be documented and communicated to the FEC OIG COTR at the time they are identified. Within one (1) week after receipt of comments from the COTR, the contractor shall submit a final management letter, which incorporates all comments from the COTR.

e. Working papers - The audit working papers are the property of the FEC OIG and are to be fully referenced and cross referenced before they are provided to the government. The working papers shall be delivered to the COTR within one (1) day after delivery of the final approved audit.

f. Progress reports/Status meetings - The FEC OIG COTR and/or IG will be provided at least one formal status briefing every two weeks regarding the progress and tentative findings of the audit team. Work paper review will also be undertaken at this meeting. Any matters that come to the attention of the audit team that could have a material impact on the financial statements are to be communicated to the COTR immediately. The COTR will then schedule a meeting between the OIG, IPA and management to discuss all findings and recommendations.

6. PERIOD OF PERFORMANCE

The task order contract shall be in effect for one base year and four option years. The period of performance for this task order shall be the date of award through December 31, 2008. Base year begins at date of award through December 31, 2004. Option periods begin on the calendar year period, January through December. Option periods shall be exercised at the discretion of FEC OIG, in accordance to FAR clauses 52.217-9 and 52.232-19.

7. PLACE OF PERFORMANCE

The contractor places of performance shall be onsite at FEC, located at 999 E Street, NW, Washington, D.C. and offsite at contractor's location based on direction of COTR assigned to contract.

8. GOVERNMENT FURNISHED PROPERTY

For onsite performance by the contractor, FEC will provide workstation facilities for contractor personnel, which includes access to telephone and office equipment including copy and fax machines. The contractor shall provide any items not furnished by FEC.

9. AUTHORIZED FEC REPRESENTATIVES

Contracting Officer's Technical Representative

Name: Jon Hatfield

Organization: Office of Inspector General, FEC
 Address: 999 E Street NW, Washington, DC 20463
 Phone Number: (202) 694-1015

The Contracting Officer's Technical Representative (COTR), to be appointed in writing by the Contracting Officer, is designated to represent the Contracting Officer for all technical matters that arise under the contract that he is assigned. The specific duties of the COTR are clearly articulated in the letter of appointment he receives from the Contracting Officer. Some of the responsibilities of the COTR include: (1) determining the adequacy of performance and/or the timeliness of delivery by the Contractor in accordance with the terms and conditions of this contract; (2) acting as the Contracting Officer's representative in charge of work at the site; (3) ensuring compliance with the contract's requirements insofar as the work is concerned; (4) advising the Contracting Officer of any factors that may cause delays in delivery and/or performance of the work; (5) reviewing and recommending approval of Contractor invoices and (6) conducting and/or witnessing the conduct of any inspections and/or tests that may be required by the contract.

Contracting Officer

Name: Jacquelyn Connell
 Organization: Federal Election Commission (FEC)
 Address: 999 E Street NW, Washington, DC 20463
 Phone Number: (202) 694-1328
 Email address: jconnell@fec.gov

The Contracting Officer has the overall responsibility for the award and administration of this contract. The Contracting Officer alone, without delegation, is authorized to take actions on behalf of the FEC Office of Inspector General to amend, modify, or deviate from the contract's terms, conditions, requirements, specifications, details, and/or delivery schedules. However, the Contracting Officer may delegate certain other responsibilities to authorized representatives.

10. SECURITY REQUIREMENTS

All contractor personnel working on FEC premises shall adhere to FEC security requirements. Presently, contractor personnel are required to wear identification badges while on-site. The contractor is responsible for assuring that ID badges, access cards, and any other Government-owned property, are promptly returned to the FEC at the conclusion of the employee's work at the site, and shall be returned at any other time upon request of the COTR.

11. TECHNICAL DIRECTION AND SURVEILLANCE

(a) Performance of work under this task order shall be subject to the surveillance and written technical direction of the COTR. The term "technical direction" is defined to include:

Technical direction must be within the scope of work. The COTR does not have authority to, and may not, issue any technical direction which:

- (1) Assigns additional work outside the Statement of Work for the order;
- (2) Constitutes a change as defined in the contract clause entitled "Changes";

(3) In any manner causes an increase or decrease in the order price or the time required for performance;

(4) Changes any of the expressed terms, conditions or specifications of the task order; or

(5) Interferes with the contractor's right to perform the terms and conditions of the task order.

(b) All technical direction shall be issued in writing by the COTR. The contractor shall proceed promptly with the performance of technical directions duly issued by the COTR in the manner prescribed in this clause and within his/her authority under the provisions of this clause. If, in the opinion of the contractor, any instruction or direction by the COTR would increase the cost of the task order or result in work outside the scope of this task order, the contractor shall not proceed but shall immediately notify the Contracting Officer in writing. It is anticipated that within 30 days of receiving the notification from the contractor, the Contracting Officer will either issue an appropriate contract modification or advise the contractor in writing that:

(1) The technical direction is rescinded in its entirety;

(2) The technical direction is within the scope of the task order, does not constitute a change under the "Changes" clause of the contract and that the contractor should continue with the performance of the technical direction.

(c) A failure of the contractor and Contracting Officer to agree that the technical direction is within the scope of the task order, or a failure to agree upon the contract action to be taken with respect thereto shall be subject to the provisions of the "Disputes" clause of the contract.

(d) Any action(s) taken by the contractor in response to any direction given by any person other than the Contracting Officer or the COTR whom the Contracting Officer shall appoint shall be at the contractor's risk.

12. TRAVEL COSTS

Costs for transportation, lodging, meals and incidental expenses incurred by contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. Should any travel be required (e.g., to the National Finance Center), a modification to the Task Order will be negotiated at the time it is required.

13. INSPECTION AND ACCEPTANCE

The Government may accept, conditionally accept, or reject any deliverables within 30 days after receipt of the item. A notice of conditional acceptance shall state any corrective action required by the Contractor. If the deliverable is rejected, the Contractor may be required, at the option of the Government, to correct any or all of the deliverable. The Government shall take action on the corrected deliverable within the time frame specified. Contracting Officer's Technical Representative shall be responsible for receipt of all deliverables.

14. KEY PERSONNEL

(a) The personnel listed in the technical proposal are considered essential to the work being performed hereunder. Prior to removing, replacing, or diverting any of the specified individuals, the contractor shall notify the Contracting Officer reasonably in advance (but not less than 30 days) and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on this task order. No diversion shall be made by the contractor without the written consent of the Contracting Officer. No increases in the firm-fixed price will be allowed because of required substitutions. Approved substitutions will be reflected in this task order by written modification.

(b) The contractor shall immediately remove any employee from performance of work under this task order, and shall expeditiously replace that employee with one deemed acceptable to the Contracting Officer's Technical Representative (COTR), upon receiving notice from the Contracting Officer that the employee's performance is unsatisfactory.

15. NON-DISCLOSURE OF CONFIDENTIAL DATA

(a) The contractor shall not divulge information obtained from the FEC to any person for any purpose, except for performance in connection with this task order; shall not directly or indirectly use or allow the use of FEC information for any purpose other than that directly associated with officially assigned duties; and shall not, either by direct action or by counsel, discussion, recommendation, or suggestion to any unauthorized person, reveal the nature or content of any FEC information. The foregoing obligations, however, shall not apply to information that--

- (1) At the time of receipt by the contractor, is in the public domain;
- (2) Is published by others after receipt thereof by the contractor or otherwise becomes part of the public domain through no fault of the contractor; and/or
- (3) The contractor can demonstrate was already in its possession at the time of receipt thereof and was not acquired directly or indirectly from the Government or other companies;
- (4) The contractor can demonstrate was received by it from a third party that did not require the contractor to hold it in confidence.

(b) The contractor shall obtain from each employee permitted access a written agreement, in a form satisfactory to the Contracting Officer, that he/she will not discuss, divulge or disclose any such information or data to any person or entity except those persons within the contractor's organization or the Government directly concerned with the performance of the task order.

16. ORGANIZATIONAL CONFLICTS OF INTEREST (OCI)

If the contractor is aware, or becomes aware during the period of performance of this task order, of any facts that might create an actual or potential conflict of interest, the contractor shall immediately provide a detailed disclosure of such facts to the Contracting Officer. At the request of the Contracting Officer, the contractor shall provide a conflict of interest avoidance or mitigation plan to the FEC. If such a plan is requested, continued performance under this task order may be conditional upon the Contracting Officer's approval of the plan.

If approved by the Contracting Officer, the conflict of interest avoidance or mitigation plan shall be deemed incorporated into this task order, pursuant to this provision. This clause shall be included in any teaming or subcontract agreements with respect to work performed under this task order.

17. GOVERNMENT RIGHTS IN SOFTWARE AND DATA

The Government shall have unrestricted rights in all computer software, documentation, and other data developed by the contractor under this task order, in accordance to FAR Clause 52.227-14, Rights in Data-General (June 1987).

18. PAYMENTS

Payments shall be rendered after acceptance of deliverables. Acceptance shall occur on the seventh calendar day after the delivery of the services in accordance with the terms of the contract.

Payments under this contract shall be made by electronic funds transfer in accordance to FAR 52.232-33.

An invoice shall be prepared and submitted to the designated billing office specified herein. A proper invoice must include the items listed in items 1-6 below. If the invoice does not comply with these requirements, the contractor will be notified of the defect within seven days after receipt of the invoice in the billing office.

1. Name and address of the contractor
2. Invoice date
3. Purchase Order Number
4. Description, quantity, unit of issue, unit price, and extended price of supplies delivered or services performed
5. Payment terms
6. Name and address of contractor official to whom payment is to be sent

Final payment will be made upon full completion and submission to the FEC of all deliverables and acceptance by the Government. Interim payments up to 80% of the total contract price will be made in accordance with a schedule submitted by the offeror, and accepted by the FEC. All payments are contingent upon receipt of an invoice in accordance with this clause, and shall be made in accordance with the clause entitled "Prompt Payment".

Attachment No. 2

Completion of mandatory FEC security awareness training, signed in May and June of 2007, by Clifton Gunderson partners and employees

Case Number INV-09-02

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, *"Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."*

Please sign and date indicating that you have attended the described training.

1	[Redacted]	[Redacted]	Clifton Gunders on LLP – FEC OIG contractor	6/18/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, *"Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."*

Please sign and date indicating that you have attended the described training.

1	[Redacted]	[Redacted]	CLIFTON GUNDERSON LLP	5/27/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, *"Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."*

Please sign and date indicating that you have attended the described training.

	Print your name	Signature	Division	Date
1	[REDACTED]	[REDACTED]	Clifton, Gunderson	5/24/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, "Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."

Please sign and date indicating that you have attended the described training.

1	[Redacted]	[Redacted]	OIG	9/6/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, "Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."

Please sign and date indicating that you have attended the described training.

	NAME	POSITION	SIGNATURE	DATE
1	[REDACTED]	[REDACTED]	CG [REDACTED]	8/9/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, "Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."

Please sign and date indicating that you have attended the described training.

1	[Redacted]	[Redacted]	014 Accounting	7/2/07
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

Please be aware that this is mandatory training for all employees and contractors. Pursuant to the Public Law 100-235, the Computer Security Act, *"Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."*

Please sign and date indicating that you have attended the described training.

1	[Redacted]	[Redacted]	OIG	5/25/07
2	[Redacted]	[Redacted]	OIG	6/18/07
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

Attachment No. 3

FEC Commission Directive No. 58, effective January 16, 2007

Case Number INV-09-02

FEDERAL ELECTION COMMISSION		
MANUAL OF DIRECTIVES	COMMISSION DIRECTIVE	
	REVOKES: November 25, 1997	NO. 58 (Revised)
	EFFECTIVE DATE: January 16, 2007	
Electronic Records, Software and Computer Usage		

Scope: The provisions contained within this directive apply to all Divisions and associated personnel of the Federal Election Commission (FEC), regardless of their position, location or relationship with the Commission. This includes, but is not limited to:

- o all authorized users who access Federal Election Commission information systems, networks, and data processing devices,
- o all vendors/contractors and their related personnel acting for the Federal Election Commission, and
- o to non-Federal Election Commission organizations, including other Government agencies, who are granted access to Federal Election Commission information resources.

This directive applies equally to mainframe, minicomputer, and microcomputer environments of the Federal Election Commission.

Only those persons who have written permission from the Federal Election Commission's Chief Information Officer are exempt from these provisions.

Direct questions concerning this directive should be directed to the Federal Election Commission's Information System Security Officer, Information Technology Division (ITD).

Definitions: The term "FEC Information System" refers to and includes any and all forms of equipment, tools and intellectual property related to computer use. This includes computer systems, personal computers, personal digital assistants, computer networks, and all forms of software, firmware, operating software and application software that the FEC owns or that is under the FEC's possession, custody or control.

The term "electronic records" refers to and includes digital images, computer-generated spreadsheets, electronic versions of paper documents, the products of desktop publishing software, e-mail and any future types of information generated on Commission automated data processing equipment and stored in Commission databases.

The term "software" includes commercial software purchased by the agency and computer programs developed by agency staff or contract personnel.

The term “sensitive information” refers to any data/information (whether in an electric or non-electric format) where loss, misuse, or unauthorized access to or modification of could seriously hamper the Commission’s ability to carry out its mandated functions. Information previously categorized as confidential is considered a subset of sensitive. Personal and Privacy Act information are classified as sensitive information.

General Policy: The Commission’s large-scale investment in computer technology has greatly enhanced our capabilities in the agency’s disclosure program, our audit and enforcement programs, and our day-to-day administrative activities. Our Information Technology Architecture (ITA) is largely decentralized and considerable autonomy is therefore afforded individual staff members (hereafter, “end users”). This, in turn, confers considerable responsibility on end users to ensure that information systems are used appropriately and protected from loss, misuse, or unauthorized access. This includes a responsibility to minimize the FEC vulnerability to inadvertent or malicious system failures, to respect software licensing and copyright laws, and to protect information stored on agency computers.

Protecting Paper and Electronic Records: Information in electronic form is no less the public’s property than is information recorded on paper. The speed and ease with which one may communicate over the computer network does not diminish the official nature of the content of such communications. FEC electronic and paper records are protected under the Privacy Act, FECA and applicable FEC Information Technology (IT) policies and standards. Paper and electronic records are accessible through the Freedom of Information (FOIA) and Sunshine Act. Consequently, these records must be safeguarded and archived with the same attentiveness, as their level of sensitivity requires. FOIA access to electronic records includes the end user’s assigned personal computer as well as other Commission’s information resources.

The FEC has developed and implemented a comprehensive entity-wide information system security program designed to protect the confidentiality, integrity, and availability of its systems, networks, and data. However, even after its considerable investment, the FEC realizes that the primary component of any security program is you the end user. As the principal component of the FEC system security program, end users take on the burden of protecting the confidentiality, integrity and availability of information when they bypass FEC security guidelines by saving your work to media other than the FEC network. As in the case of paper records, each individual user is also responsible for the erasure and/or destruction of any sensitive information the user chooses to store outside of the FEC network.

If there is any doubt as to what is considered sensitive versus non-sensitive, staff should consult their FEC Management and contracting personnel should contact their contracting officer representative. If there is any doubt as to proper protection procedures for sensitive information, staff should consult their FEC Management and contracting personnel should contact their contracting officer representative and if necessary, the FEC Information Systems Security Officer.

Control of Computer Software: Commission computers employ a variety of standardized commercial software and custom computer programs. Strict control over computer software is necessary to maintain the integrity and coherence of the agency's information technology architecture (ITA), to comply with intellectual property copyright laws and licensing agreements, and to shield FEC computers and databases from destructive computer "viruses."

ITD has implemented a process to anticipate the software needs of Commission staff across-the-board. Nonetheless, individual employees or units may have specialized needs that they believe can be satisfied with other commercially available software packages. All software, however, must be purchased, installed, and configured by ITD staff. The Training and Computer Support Branch will assist offices with unique application requirements.

Downloading "freeware" and "shareware" from the Internet is prohibited. In addition end users are also prohibited from copying agency purchased commercial software for installation on non-FEC computers.

FEC computer systems and/or user accounts are subject to inspection and monitoring for non-compliance with applicable laws, regulations, policies and procedures. There is no expectation of privacy with a government computer system and/or account.

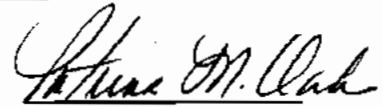
All agency computers are protected by anti-viral software, which is updated as new strains are detected and countermeasures devised. Computer viruses can wreak havoc on individual computers and the entire network. End users may not disable the anti-viral software or reconfigure operating system features. End users should alert the ITD HelpDesk immediately if they believe they have detected a viral infection on their computer despite these safeguards.

Restrictions on Use of Commission Computer Systems: End users have considerable control over the manner in which they employ their computer system and the manner in which they communicate over the internal agency network and the Internet. The following guidelines must govern that use:

- A. Do not use the system to solicit co-workers for unauthorized charities, to advertise personal property for sale, or for other personal benefit. Staff may, however, use the system to broadcast news of a personal nature of interest to their co-workers, such as birth announcements.
- B. Staff must refrain from using offensive, insensitive or intemperate language about people and issues in internal or Internet e-mail. Employees should remember that personal opinions lose any privacy protection once they are imprinted on government records be they paper or electronic. Both the end user and the agency can be held liable by an offended party.

- C. De minimis personal use of the system is acceptable just as it is with the telephone. Any such use must be appropriate, must not incur any additional costs to the government and must not impede the fulfillment of your FEC work.
- D. In the case of the personal use of Internet e-mail, you should make it clear, when appropriate, that your e-mail is not an official communication from the agency.
- E. The Internet contains material, such as sexually explicit material, that is not appropriate for the workplace. The FEC expects employees to conduct themselves professionally in the workplace and to refrain from using government resources for activities that are offensive to co-workers or the public.

This Directive was adopted on January 16, 2007.



Patrina M. Clark
Staff Director

Attachment No. 4

FEC Mobile Computing Security Policy No. 58-4.3

Case Number INV-09-02

Federal Election Commission
Mobile Computing Security Policy
Policy Number 58-4.3

1. PURPOSE

This policy is designed to:

- a. Satisfy the purposes and policy goals of the Federal Election Commission (FEC) Information System Security Program Policy, Policy Number 58A.
- b. Establish control over the processes to physically secure portable computing and communications devices (e.g., laptop computers, cell phones, personal digital assistants and other internet/two-way communications-enabled devices such as pagers) that process, store or transmit FEC information. This policy is designed to help maintain control over high-value FEC assets, and safeguard FEC information. This policy is enabled by policies, practices and devices for securing portable computing devices, and takes into consideration:
 - i. The convenience and practical advantages afforded by use of portable computing devices and their peripherals;
 - ii. The popularity of portable computing devices and their peripherals as targets for thieves;
 - iii. The vulnerability of portable computing devices and their peripherals assets to unauthorized access or theft; and
 - iv. The unique risks posed by portable computing devices and their peripherals to FEC information confidentiality, integrity and availability.

2. POLICY

It is FEC policy that:

- a. Portable computing devices and associated peripherals issued by the FEC should be viewed as government property that must be adequately protected from theft;
- b. Privately-owned portable computing devices that are used to process, store, or transmit FEC information are considered government-interest assets, and should be afforded the same anti-theft protection as agency-owned assets for as long they contain FEC information;
- c. During the normal workday, whether working in a FEC office or at an off-site location, a security cable should be used to fasten FEC laptop computers to a desk, chair or other fixed object;
- d. All portable computing devices should be locked in a secured area at the end of the workday;

- e. Portable computing devices should not be left unattended while being transported, unless locked in a secure location where not visible (e.g. airport terminal locker, the trunk of a locked car);
- f. Portable computing devices must not be checked with other baggage when traveling;
- g. If a portable computing device that contains FEC information is stolen (regardless of where the theft occurs), the device's owner/user (i.e., the person responsible), should:
 - i. Notify the Information System Security Manager (ISSM) as soon as possible; and
 - ii. File a police report as soon as possible.
- h. All assigned portable computing devices, peripherals, related equipment and media are FEC property and are to be returned to the IT Division upon request, or when an employee leaves FEC's employment;
- i. Passwords should be used to deter unauthorized access to portable computing devices re-activating from a suspended mode whenever possible. FEC's *Password Policy* is relevant here.
- j. All mobile computing devices including Blackberries and Palm Pilots must be encrypted and/or password protected.
- k. All laptops that access the FEC Local Area Network (LAN) will be required to employ a FEC provided two-factor authentication mechanism where one of the factors is a device separate from the computer gaining access.
- l. All FEC mobile computing devices must use a "time-out" function for remote access and mobile devices requiring user reauthentication after a minimum of 30 minutes inactivity.

3. RESPONSIBILITIES

- a. All FEC authorized users of FEC information:
 - i. Comply with the terms of this policy; and
 - ii. Report violations of this policy expeditiously to cognizant authority.
- b. The FEC Director, Information Technology, Chief Technology Officer:
 - i. Sign, issue, and oversee the implementation and enforcement of this policy;
- c. FEC Manager, Program Management:
 - i. Develop and issue technical standards regarding acceptable anti-theft devices; and
 - ii. Implement and manage changes to this policy.
 - iii. In coordination with Business Owners and the ISSM, help assess the actual or possible operational impact resulting from mobile computing device loss, theft or damage;

- iv. Maintain records by nomenclature and serial number of mobile computing devices that are reported as lost or stolen; and
 - v. In coordination with the ISSM, investigate cost-effective ways to reduce theft threats.
- d. The FEC Information Systems Security Manager (ISSM):
- i. Assist the FEC Manager, Program Management with implementing and managing changes to this policy; provide oversight of policy enforcement; and
 - ii. In coordination with the FEC Program Manager and Business Owners, help assess the actual or possible operational impact resulting from mobile computing device loss, theft or damage.
- e. The FEC Assistant ISSM:
- i. Assist the ISSM with implementing this policy as required.
- f. Business Owners for FEC General Support Systems and Major Applications:
- i. In coordination with the FEC Program Manager and the ISSM, help assess the actual or possible operational impact resulting from mobile computing device loss, theft or damage.
- g. Systems Owners for FEC General Support Systems and Major Applications:
- i. Report lost, stolen, or missing portable computing devices immediately in accordance with *FEC Incident Response Policy and Impact Assessment Standards*; and
 - ii. In cases where sensitive information may have been compromised, inform the ISSM.

Revision History


Revision Number	Revision Date	Revision Synopsis
1	8/24/06	Modifications to protect sensitive information
2		
3		
4		
5		
6		
7		
8		

Attachment No. 5

FEC Non-Disclosure Agreement
signed in 2007
by Clifton Gunderson partners and employees

Case Number INV-09-02

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, , as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.



Signature

Printed Name

Partner

Title

Clifton Gunderson LLP


11710 Beltsville Dr., Suite 300, Calverton, MD 20705

Company

Address

Date 08-20-07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, , as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

 
Signature Printed Name

PARTNER
Title

Clifton Gunderson LLP 4041 Powder Mill Road, Ste. 410, Calverton, MD 20705
Company Address

Date 3/12/07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, [REDACTED], as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

[REDACTED]

[REDACTED]

Signature

Printed Name

PARTNER

Title

Clifton Gunderson LLP

4041 Powder Mill Road, Ste. 410, Calverton, MD 20705


Company

Address

Date

3/15/07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I,  as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.



Signature

Printed Name

PARTNER

Title

Clifton Gunderson LLP


4041 Powder Mill Road, Ste. 410, Calverton, MD 20705

Company

Address

Date 05/24/07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, , as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.



Signature



Printed Name

SENIOR MANAGER

Title

Clifton Gunderson LLP

Company

4041 Powder Mill Road, Ste. 410, Calverton, MD 20705

Address

Date

3/13/2007

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, [REDACTED], as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

[REDACTED]	[REDACTED]
Signature	Printed Name
Manager	
Title	
Clifton Gunderson LLP	4041 Powder Mill Road, Ste. 410, Calverton, MD 20705
Company	Address
Date <u>3/15/07</u>	

FEDERAL ELECTION COMMISSION
NON-DISCLOSURE AGREEMENT

I, [REDACTED], as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

[REDACTED] _____
Signature Printed Name

Senior Consultant
Title

Clifton Gunderson LLP 4041 Powder Mill Road, Ste. 410, Calverton, MD 20705
Company Address

Date 5/24/07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, [REDACTED], as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

[REDACTED] _____
Signature Printed Name

Associate

Title

Clifton Gunderson LLP 4041 Powder Mill Road, Ste. 410, Calverton, MD 20705

Company Address

Date 3/14/07

FEDERAL ELECTION COMMISSION NON-DISCLOSURE AGREEMENT

I, [REDACTED], as an employee/subcontractor/consultant/representative of Clifton Gunderson LLP (Contractor), operating under the terms and conditions of Contract No. GS23F0135L (PO Number FE4AC0065) with the Federal Election Commission (FEC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between Clifton Gunderson LLP (Contractor) and the FEC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FEC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

[REDACTED]

Signature

[REDACTED]

Printed Name

Associate
Title

Clifton Gunderson LLP
Company

4041 Powder Mill Road, Ste. 410, Calverton, MD 20705
Address

Date 7/3/07

Attachment No. 6

FEC Nondisclosure Agreement for Contractors
signed in 2008
by Clifton Gunderson partners and employees

Case Number INV-09-02



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

Exceptions. I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

GS 23 F0135L
FE4AC 0065 (contract number)

Clifton Gunderson LLP (company)

[REDACTED] (typed/printed name)

[REDACTED] (signature)

05/30/2008 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

FE-A-AC-0065/FE-06-C-065
(contract number)

 (typed/printed name)

Clifton Gunderson LLP (company)

 (signature)

05/28/08 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

GS23F0135L (contract number)
(FE4AC0065)

[REDACTED] (typed/printed name)

Clifton Gunderson (company)

[REDACTED] (signature)

6/5/08 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

23 FOI 35L
E4 AC 0065

_____ (contract number)
_____ (typed/printed name)

CLIFION GUNDERSON (company)
_____ (signature)

6/19/08 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

GS23F0135L-(FE4AC0065)
(contract number)

[REDACTED]
(typed/printed name)

Clifton Gunderson (company)

[REDACTED]
(signature)

6/2/08 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

S&B FO135L (FE4AC0065)
(contract number)

[Redacted] (typed/printed name)

Wilton Henderson (company)

[Redacted] (signature)

6/12/2008 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

7. **Exceptions.** I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

3FC135L (FE4AC0065)
(contract number)

 (typed/printed name)

Clifton Eunders (company)

 (signature)

06/02/2009 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
 Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

Exceptions. I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

GS23 F0135L - (FE4AC0065)
(contract number)

[Redacted]
(typed/printed name)

Clifton Gunderson
[Redacted] (company)
[Redacted] (signature)

09/04/08 (mm/dd/yyyy)



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

NONDISCLOSURE AGREEMENT FOR CONTRACTORS

1. I, [REDACTED], understand and acknowledge that I may be granted access to sensitive, protected, and confidential information related to the Federal Election Commission (FEC), including, but not limited to, information about individuals, including personally identifiable information, protected by the Privacy Act and other federal laws; information pertaining to the investigation, prosecution and conciliation of enforcement matters under the Federal Election Campaign Act, the unauthorized disclosure of which is a misdemeanor; proprietary or otherwise confidential commercial information owned by other third parties, such as software vendors to the FEC; and information related to the business, personnel and security practices of the FEC. I agree to use such information only in the course of my official duties in connection with the provisions of the below referenced contract.
2. **Disclosure of FEC information.** I agree to hold the FEC's sensitive, protected, and confidential information, including personally identifiable information, in whatever form or format, in strict confidence, and to take all reasonable precautions to protect against unauthorized use or unauthorized disclosure of such information, including but not limited to compliance with the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and System Resources.
3. **Duty to report.** I agree to report immediately to an appropriate employee of the FEC any unauthorized use, unauthorized disclosure, or other breach of sensitive, protected, and confidential information of which I become aware, or which I suspect has occurred or may occur.
4. **Return of FEC material and information.** At the conclusion of my work under this contract, I will return to the FEC (or destroy, upon written approval of the Contracting Officer) all FEC material, including copies, and all records containing FEC material and information.
5. **Deactivation of Access to FEC Information System Resources.** Immediately at the conclusion of my work (no later than 1 business day) under this contract I agree to notify the FEC Information Technology HelpDesk, in writing, that I no longer require access to FEC Information Resources.
6. **Destruction of Personally Identifiable Information (PII).** Prior to final payment on the contract, I will verify with the COTR and/or contracting officer that I have destroyed any and all FEC PII that has come into my custody while working for or at the FEC. The destruction method must be consistent with FEC IT Security Policies.

Exceptions. I understand that this Agreement shall not apply to: (1) Disclosures of sensitive, protected, and confidential information approved in advance in writing by the Contracting Officer or an FEC employee who is at the Senior Level and above; or (2) Information that is or was publicly available by means other than my disclosure; or (3) Compliance with a valid court order; provided, however, that I agree to inform the General Counsel of the FEC as soon as possible after, and in no event more than one business day after, my receipt of such a court order, and to provide the General Counsel with a complete copy of the order.

7S23FO135L-(FE4AC0065)
(contract number)

[Redacted] (typed/printed name)

Clifton Anderson (company)

[Redacted] (signature)

07/26/2018 (mm/dd/yyyy)

Attachment No. 7

Letter from [REDACTED] to Alec Palmer
dated 09/05/07

Case Number INV-09-02



September 5, 2007

By email: Apalmer@fec.gov

Mr. Alec Palmer, CIO
Federal Election Commission
999 E Street, NW
Room 820 A
Washington, DC 20463

Dear Mr. Palmer

In order to prevent any delays in the audit process, we are requesting an exception to the Federal Election Commission (FEC) policy requiring that all laptop computers that remotely access or provide remote storage for sensitive information have a two-factor authentication. We are requesting the policy exception for only Clifton Gunderson laptops used in accessing and storing financial information required to support the 2007 CFO audit.

In connection with the requested remote access and storage we:

- Will remove any and all FEC data from all laptops within 90 days of the conclusion of the audit (when the final report is issued).
- Will encrypt all FEC data on all Clifton Gunderson laptops.
- Will report any instance of any and all irregularities concerning FEC data immediately.
- Will not use this computer security exception as a audit finding.

During the year, we will continue to work with Mr. Bouling to hopefully solve the glitches that were preventing the successful implementation of the two-factor authentication in Clifton Gunderson laptops.

11710 Beltsville Drive
Suite 300
Calverton, Maryland 20705
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

Offices in 15 states and Washington, DC

Member of
HLB International

FOIA 2016-32_134

Mr. Alec Palmer, CIO
Federal Election Commission
September 5, 2007
Page 2 of 2

If you have any questions, please do not hesitate to contact me at 301-931-2050 or George.Fallon@cliftoncpa.com.

Sincerely

A large black rectangular redaction box covering the signature area.

 CPA
Partner

CC: Ed Bouling, Security Officer
Erin Singshinsuk, CFO
Lynne McFarland, IG

Attachment No. 8

CG documents provided by [REDACTED] on 02/12/09:
Wireless Equipment Checkout (Ticket #1083), dated 02/02/09
and
Wireless Equipment Checkout (Log)

Case Number INV-09-02

FAX • FAX • FAX • FAX • FAX • FAX

Redaction pursuant to FOIA Exemptions 6 & 7(C)

Clifton Gunderson is the 13th largest CPA and consulting firm in the country, with offices in 15 states and Washington, DC.



Clifton Gunderson LLP
Certified Public Accountants & Consultants

Calverton Office Park
11710 Beltsville Drive, Suite 300
Calverton, Maryland 20705
301-931-2050
301-931-1710 Fax

Date: 2/12/09
Number of Pages:
(including cover)

Services

- Assurance and Accounting Services
- Corporate Finance Services
- General Business Consulting
- International Services
- Clifton Gunderson Financial Services
 - Asset Management
 - Employee Benefit Services
 - Financial Planning
 - Insurance Services
 - Retirement Planning
- Succession Planning
- Tax Consulting Services
- Tax Preparation Services
- Technology Consulting
- Valuation and Forensic Services

Accounting services offered through Clifton Gunderson LLP. Advisory services offered through Clifton Gunderson Financial Advisors, L.L.C., a Registered Investment Advisor. Fixed rate insurance products offered through CG Risk Management, L.L.C. Retirement Plan Administration services offered through CGFS Holding LLC.

To: JOEL DUCAN

Fax: 202-501-9134 Phone:

Sent By: [REDACTED]

MESSAGE:

IT

COUNT ON INSIGHT®

www.cliftoncpa.com



Clifton Gunderson LLP Fax Notice

The information contained in this facsimile transmission (and/or documents accompanying it) is confidential and is for the use only of the intended recipient. If you are not the intended recipient, any disclosure, copy, distribution or other use of this information is prohibited. If you have received this communication in error, please notify us immediately by telephone and delete or discard this message immediately. New IRS rules, which govern the way we conduct our tax practice, dictate that we give you the following notice: Any tax advice included in this communication (including attachments) is not intended or written to be used, and it cannot be used by any taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer.

Wireless Equipment Checkout

Ticket #: 1083

Checkout Date:

2/2/2009

Return Date:

Borrower Information

Name: [REDACTED]
Department:
Phone / Ext: 27040

Wireless Description

Brand: HP
Model: 0000bannor
Serial #: 2UA508087J
Asset #: 261356

Additional Items

Printer:
512 Flash Drive:
USB Hard Drive:
Network Cables:
Bag:
Network Card:
CD/DVD Drive:
Other:
Other Description: Power Cord

Scanner Description

Brand:
Model:
Serial #:
Asset #:

Borrower Signature:

[REDACTED]

Tech Signature:

Ballina

Redactions Pursuant to FOIA Exemption (b)(7)(C)



Wireless Equipment Checkout Tool

Ticket #	Name	Department	Phone	Checkout Date	Return Date	Brand	Model	Serial #	Asset #	Scanner ScanSta #	Model #	Serial #	Asset #	Printer	512 Flash Drive	USB Hard Drive	Network Cables	Bag	Network Card	CD/DVD Drive	Other	Description	Status	Date of Return	Overdue	Damaged	Missing	Damage/Missing Description	
1073	Marie Scott		27072	1/13/08		Fujitsu	6-5110C	199	261528 p	ScanSta	5110C	159		No	No	No	No	Yes	No	Yes		Power Cord							
1075	Heather Pitt		27032	12/1/09		Fujitsu	S510	13080	580142 p	ScanSta	S510	13080		No	No	No	No	Yes	No	No	No	Power Cord	Out						
1081	Dan Choi			12/2/08	12/2/08	IDEA	KEY		2 055E+09					No	No	No	No	No	No	No	No		Out						
1046	Khrista Corpus	FedGov	9842	10/1/08	11/14/08	HP	HP4250	?		Arlington													In						
1048	Khrista Corpus	FedGov	9842	10/1/08	11/14/08	Fujitsu	83269	?		Arlington													In					Paper Jam	
1048	Khrista Corpus	FedGov	9842	10/1/08	11/14/08	Staples	12540-USCC	?		Arlington												Electric Hole Puncher	In						
1049	Khrista Corpus	FedGov	9842	10/1/08	11/14/08	Linksys	EF2624V2	?		Arlington												24 Port Switch	In						
1047	Khrista Corpus	FedGov	9842	10/1/08	11/14/08	Netgear	FY5318	0sqf		Arlington												8 Port Switch	In						
1087	Alumkperik		27053	2/9/09	2/12/09	HP	72783ig	4T	261285					No	No	No	No	No	No	No	No	Power Cord	Out						
1085	Andy Lee	Federal	27048	1/9/09		HP	NC8000	5P	261322					No	No	No	No	No	No	No	No	Power Cord							
1084	Haniel West		8453	12/30/08		HP	RE4	5T	261318					No	No	No	Yes	No	No	No	No	Power Cord	Out						
1052	Carina	FedGov			12/3/08	HP	T80M283.0	2LR438P3	0	4L				No	No	No	No	No	No	No	No	Power Cord	In	12/3/08	?				
1054	Kreitzman	FedGov			12/1/08	HP	T80M283.0	2LR438P3	0	4W				No	No	No	No	Yes	No	No	No	Power Cord - Mouse - Lock	In						
1985	Greg Bussink		20727	2/4/09	2/5/09	Planar	PL1500	1254						No	No	No	Yes	Yes					In	2/5/09					
1977	Herb Danber		27023	1/23/09	2/3/09	Planar	PL1500	1254						No	No	No	Yes	Yes					In	2/3/09					
1080	Issey	Arlington	571-227-8500		1/28/09	InFocus	IN3106	00051		N/A				No	No	No	No	Yes	No	No	No	Projector	In	2/2/09	No	No	No		
1905	Michelle O'Donnell	Commercial/Non Profit	737	2/22/07		Linksys	WRT54G	D2828		Washington-02				No	No	No	No	No	No	No	No		Out						
100	[Redacted]	Admin	301-931-2080		3/6/08	Linksys	WRT54G	D2828		Washington-01	Fujitsu	5110C	159	0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No		In	3/6/08	No	No	No	
700	[Redacted]	Fed Gov	748	6/16/06		Linksys	WRT54G	D2828		CG-				No	No	No	No	No	No	No	No		Out						
1014	Greg Bussink	Commercial	27027	8/10/07		Linksys	WRT54G v5	D2854		Washington-09				No	No	No	No	No	No	No	No			In		No	No	No	
1022	Toku	Shoyens	Fed Gov	0/10/07		Linksys	WRT54G v5	D2856		CG-WA-07				No	No	No	No	No	No	No	No			In		No	No	No	
1026	Dan Zancan	Commercial		11/12/07		Linksys	WRT54G v5	D2857		CG-WA-08				No	No	No	Yes	No	No	No	No		Out						
1015	Greg Bussink	Commercial	27027	8/10/07		Linksys	WRT54G v5	D2857		Washington-08				No	No	No	No	No	No	No	No			In		No	No	No	
1006	Michelle O'Donnell		27081	2/11/08		Linksys	WRT54G	D2857		Washington-00				No	No	No	No	No	No	No	No		Out						
1023	James Gubin	Commercial		9/13/07		Linksys	WRT54G v5	D2858		cg-wa-05				No	No	No	No	No	No	No	No		Out						

Redactions Pursuant to FOIA Exemptions 6 & (C)

Asset #	Name	Department	Phone	Checkout Date	Return Date	Brand	Model	Serial #	Asset #	Scanner	Model	Serial #	Asset #	Printer	STZ Drive	Flash Drive	USB Hard Drive	Network Cables	Bag	Network Card	CD/DVD Drive	Other	Description	Status	Date of Return	Overdue	Damaged	Missing	Damage/Missing Description			
1011	Den Zancan	Commercial	750	5/7/07		Linksys	WRT54G	CDFB0EA D2858	CG- Washingt on-04	Fujitsu	5500	57543	560036	No	No	No	No	Yes	No	No	No	No		In	5/31/07	No	No	No				
1013	Ndy Oparaji	Fed Gov	715	6/19/07		Linksys	v5	CDFB0EA D2859	CG- Washingt on-03	Fujitsu	5500	57543	560036	Yes	No	No	No	No	No	No	No	No	MYE(P2Y070	In	11/14/07	No	No	No				
1008	Laura Vansuch	Commercial	752	4/20/07		Linksys	WRT54G	CDFB0EA D2860	CG- Washingt on-03	Fujitsu	5500	53226	660031	No	No	No	No	Yes	No	No	No	No		Out								
1066	Michelle O'Donnell		27061	2/6/09	2/12/09	Linksys	WRT54G	D0149FA7 4F22	CG- Washingt on-03					No	No	No	No	No	No	No	No	No Power Cord (2)	Out									
1058	Javier Castro (TCC)	FedGov			12/10/08	HP		L7056FED 304 W O																In	12/10/08							
1067	[Redacted]		27025	2/4/09		HP		L7056FED GOV7 ZM				CE0562 0		No	No	No	No	No	No	No	No	Power Cord	Out									
1038	Andy Lee		27046	11/4/06	11/5/06	HP		HP-nu8000 WWO	hp-co- 6000	HP				No	No	No	No	Yes	No	No	No		In		No	No	No					
1060	Khriss Corpuz	Arlington			2/12/09	HP		CNU41502 LS															yes Power Cord	In								
1061	Despa Mangla		27035	12/16/08	12/20/08	HP		LT056CO MM05 0P						No	No	No	No	No	No	No	No		Out									
1057	Ganella Filmons		27026	12/8/08	12/8/08	HP		LT056CO MM05 0P						No	No	No	No	No	No	No	No		Out									
1063	Kyle Kilder		27119	12/22/08		HP		LT056CO MM05 0P						Yes	No	No	No	Yes	No	No	No		Out									
1067	Akimperik		27033	1/8/09	1/12/09	HP		LT056CO MM05 0P						No	No	No	No	No	No	No	No	Power Cord	Out									
1062	[Redacted]		27043	2/7/09		HP		DC Loaner LT056CO						No	No	No	No	No	No	No	No	Power Cord	Out									
1067	Bob Curtis (Trinity)	Arlington (DH6-01G)		7/1/08	2/10/09	HP		LT056CO MM01 0P						No	No	No	No	No	No	No	No	Power Cord	Out									
1060	Elijah Adams		9625		12/11/08	HP		T60M283.0 0						No	No	No	No	No	No	No	No	Power Cord	Out								out of order per EA	
1068	PAM LINDSEY	ARLINGTON	571-227-9500 X 676		1/12/09	HP		CNU53911 78						No	No	No	No	No	No	No	No		Out									
1074	Sarah Welch for Lisa Noh	Arlington	571-227-9623		1/16/09	HP		LT056CO RE2 78						No	No	No	No	No	No	No	No	Power Cord	Out									
1059	Elijah Adams		9625		12/11/08	HP		T60M283.0 0						No	No	No	No	No	No	No	No	Power Cord	Out									
1062	[Redacted]	IT	410-453-9500		12/16/08	HP		T80M283.0 0						No	No	No	No	No	No	No	No		Out								unknown (UPSed to Steve G.	
1096	Hira Shafiqat	FedGov	9671	12/4/08	12/5/08	HP/Com		375051-001 9C															Power Cord	In								
1043	Heather Pitt			1/7/08		HP/Com		pac 786220 WVD						No	No	No	No	No	No	No	No		Out									
1089	David Harris		27036	2/11/09		HP		LT056GPA RE0 GD						No	No	No	No	No	No	No	No	Power Cord	Out									
1061	Mary Meier		27057	2/2/09		HP		LT056GPA RE0 GD						No	No	No	No	No	No	No	No	Power Cord	Out									
1071	Pam Lindsay	Arlington	571-227-9976		1/13/09	1/12/09	HP	RQ996UC #ABA 4K						No	No	No	No	No	No	Yes	Yes	Power Cord	In		1/12/09	No	No	No		Steve repaired the permanent laptop and loaner has been returned. Steve did not repair this laptop in Arlington. Laptop shipped to Timonium.		
1044	Khriss Corpuz	FedGov	9642	10/1/06	11/14/08	HP		JPLGD122 44		Arlington														In								
1042	Dayo Akinola		27074	1/8/08		HP		LT056Com m05						No	No	No	No	No	No	No	No		Out								inoperable	

Redactions Pursuant to FOIA Exemptions 6 (C)

Ticket #	Name	Department	Phone	CheckOut Date	Return Date	Brand HP (PORT PRINTER)	Model	Serial #	Asset #	Scanner	Model	Serial #	Asset #	Printer	512 Flash Drive	USB Hard Drive	Network Cables	Bag	Network Card	CO/VO Drive	Other	Description	Status	Date of Return	Overtime	Damaged	Missing	Damage/Missing Description	
1066	Dan Minger	FedGov		1/7/09																		Out							
1090	George Fallon	IT	27018	8/28/08		Planar	PL1500														Yes	Monitor	Out						
1033	Andrew Lee			10/14/08																									
1029	Andy Lee	Fed Gov	27048	3/3/08						Fujitsu	S510	11767	251827	No	No	No	No	Yes	No	No	No	Yes	IDEA Key #2054630625	In	11/17/08	No	No	No	
1062	Andy Lee			12/17/08		Idea Key	2.055E+08																Out						
1012	Dan Zancan	Commercial	ext 750	8/15/07	11/26/08					Fujitsu	S500	53198	660029	No	No	No	No	Yes	No	No	No	No	Out						
1019	Dan Zancan	Commercial		8/30/07																		Yes	560080	Out					
1021	Dayo Awe	FCC		9/5/07						fujitsu	S500	53248	380030	No	No	No	No	Yes	No	No	No	No	Out						
1004	Dotie James			10/14/08																	Yes	IDEA Key # 857894508	Out		No	No	No		
1002	[REDACTED]	Admin	27071	10/3/08	10/5/08	Fujitsu	614890			Fujitsu	S510			No	No	No	No	No	No	No	No	No	Out	10/5/08					
1041	Gehrig			27087	11/5/08	Fujitsu	614890			Fujitsu	S510	614890		No	No	No	No	No	No	No	No	No	Out						
1020	Greg Bussink	Commercial		8/30/07																		Yes	560061	Out					
1035	Greg Bussink	Commercial	27027	10/17/08						Fujitsu	S510	614881		No	No	No	No	No	No	No	No	No	Out						
1078	Jessica Everard	Tax		1/29/09																	Yes	Portable Monitor	Out						
1039	Jin Lee	FedGov		11/5/08						Fujitsu				No	No	No	No	No	No	No	No	No	Out						
1040	Jin Lee	FedGov		11/5/08		Planar	PL 1500							No	No	No	No	No	No	No	Yes	Monitor p70276je104 48	Out						
1027	Joe Amnick	Fed Gov		11/20/07						Fujitsu	S110C	8009159	281336	No	No	No	No	Yes	No	No	No	No	Out						
1026	Campbell	Assurance		10/22/08						Fujitsu	S510	618885		No	No	No	No	Yes	No	No	No	No	Out						
1080	Khriss Carpuz	FedGov	9542	10/1/08	11/14/08	D-Link	D20544A0 14284															No	5 Port Switch Hub Infocus Projector	In					
1076	Kinton Dwiings	HR		1/22/09										No	No	No	No	No	No	No	No	No	Out						
1017	Laura Vansuch	Commercial		8/29/07										No	No	No	No	No	No	No	Yes	560063	Out						
1010	Linda Wyr	FCC	740	4/24/07																			10 Days Awe 9/5/07	No	No	No	No		
1025	Marie Caputo	PBOC		10/18/07						Fujitsu	S500	58750	281753	No	No	No	No	Yes	No	No	No	No	In						
1018	O'Donnell	Commercial		8/27/07						ScanSnap	S400	53328	580031	No	No	No	No	Yes	No	No	No	No	Out						
1016	Mike Crabtree	Commercial		8/29/07										No	No	No	No	No	No	No	Yes	580064	Out						
1001	Morgan Nichelle	Fed Gov	x 744	5/1/06						Fujitsu	fi-5 (110c	189	281536	No	Yes	No	No	No	No	No	Yes	261537	Out						
1028	Jefferson Nichelle	Admin	27041	2/10/06						Fujitsu	S510	48598	590153	No	No	No	No	Yes	No	No	No	No	In	10/2/08	No	Yes	No	sent to Steve Grace	
1031	Jefferson Nichelle	Admin	27041	10/2/08						Fujitsu	S510	614881		No	No	No	No	No	No	No	No	No	Out						
1072	Patricia Daniels Remy	ARLINGTON	9643	571227-	1/12/09	Fujitsu															Yes	Power Cord	In	1/12/09	No	No	No		
1024	Johansen	Commercial		10/1/07						Fujitsu	S500	53200	560032	No	No	No	No	Yes	No	No	No	No	Out						
1069	REBECCA COLLIER	ARLINGTON		571-227-8500 X 872	1/12/09					SCANSN AP S510	S510	46387	590159	No	No	No	No	No	No	No	No	No	Out						
1070	REBECCA COLLIER	ARLINGTON		571-227-8500 X 872	1/12/09					SCANSN AP	S510	53289		No	No	No	No	No	No	Yes	No	No	In						
1009	Boatling Thomas	GAO	714	4/20/07						Fujitsu	S300	53240	580028	No	No	No	No	Yes	No	No	No	No	Out	3/9/09	No	No	No	Returned by Sarah Welch.	
1053	Castro	FedGov			12/3/08	HP	T80M283.0 0		281301														In						

Ticket #	Name	Department	Phone	Checkout Date	Return Date	Brand	Model	Serial #	Asset #	Scanner	Model	Serial #	Asset #	Printer	USB			Network Cables	Network Bag	Network Card	CD/DVD Drive	Other	Description	Status	Date of Return	Overdue	Damaged	Missing	Damage/Missing Description
															512	Flash Drive	Hard Drive												
1006	Toju Shoyemi	Fed Gov	736	3/30/07						Fujitsu	S110C	159	261536	No	No	No	No	No	No	No	No	No		In	11/20/07	No	No	No	
1007	Tram Jewett	PBGC		4/19/07						Fujitsu	S-500	53200	560032	No	No	No	No	No	No	No	No	No		Out		No	No	No	
1037	Yan Zhang		27089	10/23/08	2/10/09	Fujitsu	614890			Fujitsu	S510	614861		No	No	No	No	No	No	No	No	No		Out					
1002	Zack Greene	Commercial	x 731	5/22/06										No	Yes	No	No	No	No	No	No	No	261548	In	5/23/06	No	No	No	
1003	Zack Greene	Commercial	731	5/24/06										No	Yes	No	No	No	No	No	No	Yes	261549	In	5/31/07	No	No	No	

Attachment No. 10

Fax from Roy Connor, FCC OIG
showing log screen shot for Pointsec installation

Case Number INV-09-02

Attachment No. 11

FEC OIG Contractor Security Standards

Case Number INV-09-02

FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FEC OIG Contractor Security Standards

MAY 2009

These Federal Election Commission (FEC) Office of Inspector General (OIG) Contractor Security Standards identify the minimum security standards and procedures that must be followed when accessing or storing FEC information using either FEC or contractor systems or networks. These OIG standards are intended to supplement FEC standards; where differences exist between the FEC and the OIG's standards, the highest level of security standards shall prevail. The contractor is responsible for compliance with the terms of these Standards by its employees or agents.

1. Definitions

The following definitions apply to these Standards:

“agreement” means an agreement between the FEC OIG and a contractor under which (i) the contractor performs services for the Office of the Inspector General (e.g., service provided under contract or task order from GSA schedule), or (ii) is otherwise provided access to data, confidential information, network, environment system and/or file back-up.

“computer” means any desktop or laptop computer, mobile device (e.g., cellular phone, BlackBerry), server and/or storage device that (i) may be used to access a network or environment, or (ii) may access or store data or other confidential information.

“confidential information” includes all environments, passwords, personally identifiable information (PII), and other non-public data or sensitive data.

“contractor” means any entity (including its employees and agents) that (i) performs services for the FEC OIG or as a subcontractor to a prime contractor, or (ii) is granted access to a network, FEC data or environment.

“data” means any information that resides on a network, in environments or on computers and includes any PII or other confidential information about the FEC, FEC vendors, suppliers, and employees.

“environment” means any development, test, stage and/or production computing environments to which a contractor is provided access under an agreement.

“network” means any computer network to which contractor is provided access in connection with an agreement and/or any contractor's computer networks used to provide services to the FEC OIG.

“personally identifiable information” or “PII” means information which can be used to distinguish or trace an individual's identity either directly (such as their name, social security number, biometric records, etc.) or indirectly when combined with other personal or identifying information which is linked or linkable to a specific individual (such as date and place of birth, mother's maiden name, etc.).

2. Use of Networks, Computers and Environments

Minimum System Security Standards

The following are the minimum security standards accepted by the FEC with respect to computers and other mobile computing devices.

- All laptops that access the FEC Local Area Network (LAN) will be required to employ a two-factor authentication mechanism where one of the factors is a device separate from the computer gaining access.
- All laptops that access the FEC LAN will be required to employ whole hard drive encryption.
- All mobile computing devices used to provide service under this agreement (i.e. BlackBerries and Palm Pilots) must be encrypted and/or password protected.
- All mobile computing devices must use a “time-out” function for remote access and require user re-authentication after a minimum of 30 minutes inactivity.

If the contractor is unable to supply its staff with computers or mobile computing devices that meet the minimum security standards above:

- The contractor may not use the computers or other devices to access FEC systems or data.
- The contractor may not transport, process or store *any* FEC data on the computers.
- The FEC may supply computers that comply with the minimum security standards above.

Network Protocols

Contractor is required to take the following steps to protect its own network/computers containing FEC data or when accessing an FEC network or environments, to include the following:

- Employ an industry standard Network Intrusion Detection System (NIDS) to monitor and proactively block suspicious network traffic from reaching Contractor’s network or environments.
- Manage and monitor all routers and firewall logs for unauthorized access to contractor’s network.
- Use router rules, access control lists and segmentation on any networks from which the environments or other confidential information are accessed.
- When accessing the FEC’s network over the internet, contractor may use only encrypted network traffic via industry standard Virtual Private Network (VPN).

- Contractor will use only authorized access methods such as VPN and the minimum authentication and security measures described above at all times for logical connection to the FEC networks.
- Contractor may not permit wireless access to FEC networks, computers or environments at any time.
- Contractor may transmit or make available confidential information over the internet only in an encrypted format (e.g., using https or ftps).

Access to Networks and Environments

FEC networks and the environments may be accessed only:

- if expressly permitted under the contractor's agreement with the FEC OIG;
- by contractor's employees and agents providing services under the agreement; and
- on a least-privilege basis for performance of services.

Contractor will implement physical, administrative and technical measures that restrict the ability to download, copy and/or export data only to those authorized users who are required to process the data for the performance of the services. Upon termination of service, the contractor will also implement appropriate measures to restrict the ability to download, copy and/or export the one copy of FEC data retained as required by professional standards or other legal requirements regarding the service performed; access to the data, such as audit files and workpapers, must be limited to Audit Partner or other senior management personnel.

Passwords

Contractor must maintain the following password standards for all computers, networks and environments:

- Passwords must conform to strong password standards that include length, complexity, and expiration. Passwords must not be written down or stored on-line unencrypted. Any password stored on-line must be stored using a minimum of 128-bit encryption.
- Passwords may not be shared. Each contractor employee or agent to whom access is granted must be provided a unique identifier and password.
- Contractor will abide by any further requirements for passwords as described in the *Federal Election Commission Password Standards*.

Terminating Access

Within 24 hours of termination, separation or resignation of any contractor employee or agent, the contractor must take appropriate actions to terminate his or her access to computers, networks, and environments, as well as physical access to service locations (contractor office environments). If termination, separation or resignation occurs during the agreement period of

performance, the contractor must also notify within 24 hours the FEC OIG to ensure access to FEC systems is terminated. Further, the contractor is responsible for retrieving from the employee or agent any FEC supplied property such as: security badge, building access key (Kastle Key or other keys to rooms or storage areas), computers, and/or any other issued equipment.

Logging

Contractor will retain security related logs for its computers and networks (including without limitation firewall, NIDS, operating system, VPN, and application logs) for at least 30 days.

3. Physical Security

Contractor is required to maintain the following physical security standards to prohibit unauthorized physical access at its offices at which confidential FEC information may be stored or from which FEC information, networks or environments may be accessed:

- Access must be limited to contractor employees and authorized visitors.
- Visitors must be required to sign a visitor's register and be escorted or observed when on the premises.
- Contractor must monitor and properly manage the possession of keys and access cards and the ability to access the location of FEC data (i.e. computer data center).
- When visiting or working at the FEC, contractor is required to abide by FEC building security requirements and any direction provided by FEC security staff.
- Any after-hours access to contractor premises is monitored and controlled by security.

4. Computer protection

Computer Virus Controls

Contractor will employ the following computer virus controls for all computers used to provide services under its agreement with the FEC OIG:

- Scan all e-mail sent both to and from any recipient for malicious code and delete email attachments that are infected with known malicious code prior to delivery.
- Use industry-standard virus protection software. Virus definitions must be updated regularly (in no event to exceed 7 days).
- Use automated virus updates, which may not be disabled.

Patches

Operating system security patches and software security patches must be applied promptly, when issued, on all computers. Computers should be configured to automatically receive security patches when issued.

5. Storage, Return and Deletion of Information

Storage

The contractor may not store PII, data, confidential information or environments on its computers unless required for the performance of services under an agreement. When considering whether the information is required to be stored on its computers, even on a temporary basis, the contractor should first determine whether the information can be accessed, reviewed and stored at the FEC under secure conditions. Any such information stored on computers must be permanently deleted (i.e. wiped) from a computer, in a manner that ensures that it cannot be accessed or read, as such storage is no longer required for the performance of services. All FEC data must be wiped from portable laptops and devices no later than 60 days after contract termination and contractor shall provide written certification when data removal is completed.

Removable Media and Encryption

Contractor may not store PII, passwords, data or confidential information on removable media unless required for the performance of services under an agreement. Any such information on removable media must be stored using a minimum 128-bit encryption. Information must be permanently deleted from removable media, in a manner that ensures that it cannot be accessed or read, as soon as such storage is no longer required for performance of the services.

Return and Deletion

Upon termination of services or upon request by the FEC OIG, contractor must promptly (i) return to the FEC all PII, data, environments, and (ii) delete all PII, passwords, data and environments in its possession or control (on computers or in whatever other form or media) in a manner that ensures that they cannot be accessed or read. Contractor may retain a copy of the foregoing materials for so long as required by professional standards or legal requirements, provided that any such copy is kept in an encrypted and secure format and is not used or accessed for any other purpose.

Contractor will dispose of documents containing PII, passwords, data or other confidential information only in secure shredding bins designated for sensitive or confidential information, with appropriate processes to assure that the documents are destroyed in a manner that ensures they cannot be re-created, accessed or read.

6. Business Continuity and Disaster Planning/Response

Back-up and Retention of Data

Contractor agrees to complete back-up and retention of all data as required for the performance of the services. Rules for frequency of back-ups and retention cycles shall be made available to the FEC OIG upon request. All back-ups must be stored securely.

Incident Notification and Support

Contractor shall notify the FEC OIG promptly of any incident that requires execution of the business continuity program and affects the function of computers and/or the availability or integrity of the data. Contractor will resume operations promptly after such an incident.

7. Confidentiality

The passwords for the networks and the environments, and all PII and other data are FEC confidential information. Contractor will provide its employees and agents access to the networks, environments and any confidential information only on a need to know basis, and may not disclose any confidential information to any third party without the FEC OIG's prior written consent.

8. Privacy and Data Protection

Unless required to provide the agreed services to the FEC OIG, the contractor will take reasonable steps to ensure it does not accept and retain PII and confidential data in any form. Contractor agrees that it will take the following measures to assure protection of PII and/or confidential data obtained in performing the agreed service for the FEC OIG:

- Access, use and process PII and other data only on behalf of the FEC OIG and only for the purpose specified in the Contractor's agreement with the FEC OIG, in compliance with these Standards and such further instruction as the FEC may provide regarding the processing of such PII or other data.
- Inform the FEC OIG promptly if contractor has reason to believe that legislation applicable to contractor (or changes in legislation applicable to contractor) prevent it from fulfilling the obligations related to the treatment of PII or other data under these Standards and/or contractor's agreement with the FEC.
- To the extent permitted by law, notify the FEC OIG promptly and act upon instruction concerning:
 - Any request for disclosure of the PII or other data by law enforcement or other governmental authority;
 - Any request by law enforcement or other governmental authority for information concerning processing of PII or other data in connection with the agreement between the contractor and the FEC OIG; and
 - Any request received directly from an individual concerning his/her PII.
- Abide by all federal data privacy laws and regulations applicable to the contractor's access to PII, including FEC policies and procedures on protecting PII.

9. Reporting and Responding to Security Incidents and Breaches

Contractor must immediately report to the FEC OIG (i) any security breach or other event that creates reasonable suspicion of unauthorized access to PII, data, confidential information or an environment and/or misappropriation or alteration of any PII, data or confidential information, and/or (ii) the loss or theft of any computer, whether issued by the FEC or belonging to the contractor but containing FEC data. Contractor will take appropriate steps to immediately address such incident, and will follow any additional instructions the FEC provides with respect to such incident and/or remediation identified in the response to such incident.

10. Personnel

All contractor employees and agents must be required to execute written confidentiality agreements that are consistent with the confidentiality obligations in these Standards and to comply with polices designed to prevent the disclosure of confidential information. Contractor is also responsible for assuring that its employee’s and agent’s access, use, and protect the security of service locations, computers, networks, PII, data, environments and other confidential information in a manner consistent with the terms of its agreement with the FEC and these Standards.

Contractor will employ clean desk and clear screen policies (i.e., policies and practices designed to restrict physical and logical access to confidential information on a need to know basis) to protect all data and other sensitive information.

11. Training

Pursuant to the Public Law 100-235, the Computer Security Act, *"Each agency shall provide mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."* The FEC applies this same security standard to its contractors. All contractor staff must complete FEC security awareness and privacy awareness training before being granted access to FEC systems and data.

12. Verification, Monitoring and Audit

Contractor will maintain a complete list of all individuals with permission to access the FEC and contractor network, environments and/or data. If requested, contractor will provide written response to any questions that the FEC OIG submits regarding the contractor’s security practices.

The FEC OIG may monitor the contractor’s access to and use of the environment and networks. The FEC OIG may also have security audits performed upon reasonable notice to confirm compliance with these Standards.

I have read the “**FEC OIG Contractor Security Standards**” attached hereto. I understand and agree to comply with them. The computer equipment proposed to perform the agreed service **does/does not** meet the *Minimum System Security Standards* described in section 2 above.

Contractor Name (Typed or Printed)

Name of Company (Typed or Printed)

Signature

Date

Attachment No. 12

Minimum Contractor System Security Standards
prepared by the CIO and ISSO, and incorporated into
the FY 2009 FEC OIG financial statement audit contract,
Exhibit D – “FEC Clauses & Special Provisions”

Case Number INV-09-02

EXHIBIT D - FEC CLAUSES & SPECIAL PROVISIONS

"SERVICE RELATED AWARDS" under GSA & SEWP ORDERS

- b) Contractor employees may begin work on any day of the week, as directed by the COTR, but will be required to sign in and obtain a visitors badge on a daily basis until an official FEC Badge is obtained. Until the badge is obtained contractors will not have access to ANY information technology services, hardware, online access (e.g., username and password).
- c) In addition until contractors are processed through the Security Officer and applicable FEC IT training requirements have been met access will be denied.

C. RESERVED

D. Data Breaches. The contractor shall comply with all contractual and Federal information security, privacy and confidentiality requirements applicable to the operation, maintenance or support of a Federal information system this includes FEC internal IT security policies.

1) The contractor shall be required to prevent and remedy data breaches and to provide the FEC with all necessary information and cooperation, and to take all other reasonable and necessary steps and precautions, to enable the FEC to satisfy its data breach reporting duties under applicable law, regulation, or policy in the event, if any, that a breach occurs.

2) Special attention should be paid to OMB Memorandum 06-19 (July 12, 2006), particularly the extremely urgent reporting time frames included therein for certain breaches, as well as to any other subsequent laws, regulations, or policy governing data breaches that may arise during the performance of the contract.

22. MINIMUM CONTRACTOR SYSTEM SECURITY STANDARDS: The following are security standards with respect to non-Federal Election Commission(FEC) laptop computers. This standard applies to all non-FEC contractor laptops whether accessing the FEC LAN or attempting to obtain Internet access.
- A. All laptops that access the FEC Local Area Network(LAN) are required to utilize antivirus software and have a documented process for ensuring that virus definition files are kept up to date.
 - B. All laptops that access the FEC LAN are required to apply and maintain up to date security patches for Operating system.
 - C. All laptops that access the FEC LAN are required to employ a two-factor authentication mechanism where one of the factors is a device separate from the computer gaining access.
 - D. All laptops that access the FEC LAN are required to employ whole hard drive encryption.
 - E. All laptops must use a "time-out" function for remote access and require user re-authentication after a minimum of 30 minutes inactivity.
 - F. All FEC data must be wiped from any Non-FEC laptop no later than 60 days after contract termination (FEC Information System Security 58-4.2 Media Management and Media Disposal Standards are relevant here). The contractor will provide the Contracting Technical Representative (COTR) with written certification when data removal is completed.

If the contractor is unable to supply its staff with computers that meet the minimum security standards above:

The contractor may not use the non-FEC issued computers to access FEC systems or data.

The contractor may not transport, process or store any FEC data on the non-FEC computers.

The FEC may supply computers that comply with the minimum security standards stated above.

CONTACTING THE OFFICE OF INSPECTOR GENERAL

The success of the OIG mission to prevent fraud, waste, and abuse depends on the cooperation of FEC employees (and the public). There are several ways to report questionable activity.



Call us at **202-694-1015** (a confidential or anonymous message can be left 24 hours a day/7 days a week) **or toll-free at 1-800-424-9530** (press 0; then dial 1015 - Monday - Friday 8:30am – 5:00pm).



Write or visit us - we are located at:

**Federal Election Commission
Office of Inspector General
999 E Street, N.W., Suite 940
Washington, D.C. 20463**

Mail is opened by OIG staff members only.



You can also fax (202-501-8134) or contact us by e-mail at: **oig@fec.gov**.
Website address: **<http://www.fec.gov/fecig/fecig.shtml>**

Individuals may be subject to disciplinary or criminal action for knowingly making a false complaint or providing false information.



FEDERAL ELECTION COMMISSION
 WASHINGTON, D.C. 20463
 Office of Inspector General

CLOSING MEMORANDUM

Case #: INV-10-01 (HL-10-01)	Prepared By: Joseph Duncan
Case Title: [REDACTED]	
Date of Report: 04/19/10	
Subject: Unauthorized Use of an FEC-paid Parking Permit	

This investigation was initiated based on a hotline complaint received September 24, 2009. The complaint alleged that [REDACTED], [REDACTED], accessed the FEC garage with [REDACTED] supervisor's Kastle keycard, and then displayed a "counterfeit" FEC-paid parking permit, so [REDACTED] could park [REDACTED] car in the garage. An additional allegation arose that [REDACTED], made a duplicate of [REDACTED] FEC-paid parking permit, which [REDACTED] gave to [REDACTED] along with his Kastle keycard.

The allegations were investigated to determine whether [REDACTED] and [REDACTED] misused government property, in violation of an ethical standard, title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). The investigation substantiated the allegations against [REDACTED], who admitted that in August 2009, [REDACTED] reproduced his FEC-paid parking permit and gave the duplicate permit and [REDACTED] Kastle keycard to [REDACTED], so [REDACTED] could park [REDACTED] vehicle in the FEC garage. [REDACTED] admitted that [REDACTED] was not authorized to duplicate [REDACTED] FEC parking permit. The OIG concluded that [REDACTED] improperly used FEC resources, in violation of title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). The investigation did not find administrative misconduct, only poor judgment, by [REDACTED].

OIG Disposition:

The OIG issued a report of investigation to the Commission on January 15, 2010. In the report, the OIG recommended that clear and comprehensive parking and Kastle key-card policies be implemented and widely disseminated to all FEC employees. The OIG also recommended that the garage parking attendant be provided a list of vehicles and drivers authorized to park in the garage. The OIG met with the Acting Staff Director and discussed the findings in the report. No further investigative activity is required. Therefore, this investigation is closed.

Concurrence:

Jon Hatfield, Deputy Inspector General

Date



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Lynne A. McFarland *QA for LAM*
Inspector General

SUBJECT: Report of Investigation: Unauthorized Use of an FEC-paid Parking Permit

DATE: January 15, 2010

This memorandum transmits the Office of Inspector General's (OIG) Report of Investigation: *"Unauthorized Use of an FEC-paid Parking Permit,"* dated January 15, 2010. This investigation was initiated based on a hotline complaint received September 24, 2009. The complaint alleged that on the morning of September 15, 2009, [REDACTED] accessed the FEC garage with [REDACTED] supervisor's Kastle keycard, and then displayed a "counterfeit" FEC-paid parking permit, so [REDACTED] could park her car in the garage. The parking attendant reported the incident to a Commissioner, who happened to be in the garage around the time of the occurrence.

Additional allegations arose that [REDACTED]'s supervisor, [REDACTED], made a duplicate of [REDACTED] FEC-paid parking permit, which [REDACTED] gave to [REDACTED] along with [REDACTED] Kastle keycard. The allegations were investigated to determine whether [REDACTED] and [REDACTED] misused government property, in violation of an ethical standard, title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property).

Our investigation substantiated the allegations against [REDACTED], who admitted that in August 2009, [REDACTED] reproduced [REDACTED] FEC-paid parking permit using [REDACTED] office scanner and color printer. On September 14, 2009, [REDACTED] gave the duplicate permit and [REDACTED] Kastle keycard to [REDACTED], so [REDACTED] could park [REDACTED] vehicle in the FEC garage, to attend an evening comedy hour event at the Warner Theater on September 15, 2009. [REDACTED] admitted that [REDACTED] was not authorized to duplicate [REDACTED] FEC parking permit. The OIG concluded that [REDACTED] improperly used FEC resources, in violation of title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). Because [REDACTED] has plans to [REDACTED] this month, we make no recommendations regarding his actions.

Our investigation substantiated the allegations that [REDACTED] used [REDACTED] supervisor's keycard to access the FEC garage, and then displayed a "counterfeit" parking permit to secure a parking space for [REDACTED] vehicle. However, [REDACTED] concluded that these acts did not constitute administrative misconduct because [REDACTED] supervisor improperly authorized [REDACTED] use of the permit and keycard. Because we found no administrative misconduct, only poor judgment, by [REDACTED], we recommend that [REDACTED] be counseled regarding proper parking and keycard usage.

Based on the findings in this investigation, we are troubled by deficiencies in building security access and parking controls. We are recommending that a clear and comprehensive FEC parking policy be implemented and widely disseminated to all FEC employees. This policy should include FEC-issued permit application requirements; priority of parking assignments; updating vehicle information requirements; permit display requirements; temporary permit justifications; permit transfer restrictions; and prohibitions on falsifying, forging, counterfeiting, altering, or reproducing permits, or permit applications. This parking policy should provide for the loss of parking privileges and other consequences if procedures are violated. We also recommend that the garage parking attendant be provided a list of vehicles and drivers authorized to park in the garage.

Moreover, to enhance security measures, we are recommending a clear and widely disseminated policy that governs the issuance and use of Kastle keycards to gain access to the FEC building. This policy should prohibit the sharing, transfer, or unauthorized use of keycards. It should also provide a process to ensure that users of all active keycards are accurately identified; and lost or stolen keycards are promptly reported and deactivated.

My staff will be meeting with the Acting Staff Director to discuss these findings and recommendations. If you have any questions regarding the investigative report, please do not hesitate to contact me at 202-694-1015. Thank you.

cc: Alec Palmer, Acting Staff Director



FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

Report of Investigation



Unauthorized Use of an FEC-paid Parking Permit

Case Number INV-10-01

January 15, 2010

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

OIG No ___ of ___

<u>Table of Contents</u>		<u>Page</u>
I.	Executive Summary	1
II.	Background	2
III.	Scope	4
IV.	Allegations	5
V.	Investigation Details	5
A.	Allegations Against [REDACTED] [REDACTED]	
	Allegation 1: [REDACTED] reproduced [REDACTED] <u>FEC-issued parking permit.</u>	5
	Allegation 2: [REDACTED] allowed [REDACTED] [REDACTED] to use [REDACTED] <u>FEC keycard, and a duplicate copy of [REDACTED] parking permit, to access the FEC garage and park [REDACTED] vehicle.</u>	6
B.	Allegations Against [REDACTED] [REDACTED]	
	Allegation 3: [REDACTED] [REDACTED] displayed a <u>“counterfeit” FEC-paid parking permit to secure a parking space for [REDACTED] vehicle in the building garage.</u>	10
	Allegation 4: [REDACTED] [REDACTED] accessed the <u>FEC building garage using an FEC issued keycard assigned to [REDACTED] supervisor, [REDACTED] [REDACTED].</u>	13
VI.	Findings	14
VII.	Recommendations	15
VIII.	Privacy Act and Freedom of Information Act Notice	16
	Attachment List	17

I. EXECUTIVE SUMMARY

On September 24, 2009, the Office of Inspector General (OIG) received a complaint alleging that on the morning of September 15, 2009, [REDACTED] [REDACTED] [REDACTED] [REDACTED], displayed a “counterfeit” FEC-paid parking permit to the LAZ Parking attendant, in order to park [REDACTED] car in the FEC garage. The complaint further alleged that on the day in question, [REDACTED] accessed the garage using a Kastle Systems’ keycard assigned to [REDACTED] supervisor, [REDACTED] [REDACTED]. According to the complaint, the garage parking attendant confiscated the “fake” permit and reported the incident to a Commissioner, who happened to be in the garage at the time the incident occurred.

During preliminary inquiries, the OIG uncovered allegations against [REDACTED] supervisor, [REDACTED] [REDACTED]. First, [REDACTED] allegedly reproduced [REDACTED] FEC parking permit; and secondly, [REDACTED] allegedly let [REDACTED] use [REDACTED] FEC issued Kastle keycard and a duplicate copy of [REDACTED] FEC parking permit. Based on these allegations, the OIG initiated an investigation to determine whether [REDACTED] and [REDACTED] misused government property, in violation of an ethical standard, title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property).

As to [REDACTED] our investigation substantiated the allegations. [REDACTED] admitted that in August 2009, [REDACTED] reproduced [REDACTED] FEC-paid parking permit using [REDACTED] office scanner and color printer. We found that on September 14, 2009, [REDACTED] gave the duplicate permit and [REDACTED] Kastle keycard to [REDACTED] so [REDACTED] could park [REDACTED] vehicle in the FEC garage on the following day, to attend an evening comedy hour event at the Warner Theater. [REDACTED] admitted [REDACTED] was not authorized to duplicate [REDACTED] FEC parking permit.

The OIG concluded that [REDACTED] made improper use of FEC resources, by duplicating [REDACTED] FEC-issued parking permit; and by loaning [REDACTED] FEC-issued keycard and duplicate permit to [REDACTED]. We believe [REDACTED] improper use constitutes a violation of title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). Because [REDACTED] has plans to retire this month, we make no recommendations regarding [REDACTED] actions.

Our investigation further substantiated the allegations that [REDACTED] used [REDACTED] supervisor’s keycard to access the FEC garage, and then displayed a “fake” parking permit to secure a parking space for [REDACTED] vehicle. However, we concluded that these acts did not constitute administrative misconduct because [REDACTED] supervisor improperly authorized [REDACTED] use of the permit and keycard.

We concluded that the FEC lacks a parking policy prohibiting the reproduction, transfer, or unauthorized use of FEC-paid parking permits. We further concluded that a Commission Bulletin from 2002, which prohibited the unauthorized transfer of Kastle keycards, needs to be updated and/or better disseminated to employee keycard holders. Because we found no administrative misconduct, only poor judgment, by ██████████ we recommend that ██████ be counseled regarding proper parking and keycard usage.

Based on the findings in this investigation, we are troubled by deficiencies in building security access and parking controls. We are recommending that a clear and comprehensive FEC parking policy be implemented and widely disseminated to all FEC employees. This policy should include FEC-issued permit application requirements; priority of parking assignments; updating vehicle information requirements; permit display requirements; temporary permit justifications; permit transfer restrictions; and prohibitions on falsifying, forging, counterfeiting, altering, or reproducing permits, or permit applications. This parking policy should provide for the loss of parking privileges and other consequences if procedures are violated. We also recommend that the garage parking attendant be provided a list of vehicles and drivers authorized to park in the garage.

Moreover, to enhance security measures, we are recommending a clear and widely disseminated policy that governs the issuance and use of Kastle keycards to gain access to the FEC building. This policy should prohibit the sharing, transfer, or unauthorized use of keycards. It should also provide a process to ensure that users of all active keycards are accurately identified; and lost or stolen keycards are promptly reported and deactivated.

II. BACKGROUND

The federal ethical standard on the use of government property requires FEC employees “to protect and conserve government property, and prohibits its use for other than authorized purposes.” The definition of “authorized purposes” generally includes “... those purposes authorized in accordance with law or regulation.” The regulation defines “government property” to include leasehold rights and property interests, which were purchased using Government funds.¹

¹ 5 C.F.R. § 2635.704

Federal security regulations require agencies to protect the real estate they occupy, including the protection of persons within the property.² Agency responsibilities include adhering to minimum-security standards concerning parking and entry access controls. One of these minimum security standards, “*Control of Parking Facility*” [requires that]... [a]t a minimum, authorized parking spaces and vehicles should be assigned and identified.”³

Federal facility management regulations require that privately owned vehicles parking on federally owned or leased property must display a parking permit.⁴ Under these regulations, drivers entering federal property “*are prohibited from parking on Federal property without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons... is prohibited.*”⁵

With General Services Administration (GSA) approval, federal agencies are required to regulate and police parking facilities.⁶ An agency is permitted to delegate this responsibility to parking management contractors⁷, as is the case for the FEC. However, parking spaces available to agency employees must be assigned in the following priority: a) disabled employees; b) executive personnel and those with unusual work hours; c) vanpool/carpool vehicles; d) private vehicles used for government business; and e) other private vehicles on a space available basis.⁸

The FEC leases 25 parking spaces in the building garage through an annual contract with LAZ Parking, LLC (LAZ PARKING). The monthly cost per parking space is \$230.53. The total monthly cost for all 25 parking spaces is \$5,763.25, plus a \$250 monthly “after hours” garage fee. The negotiated contract with LAZ PARKING provides four additional parking spaces to the FEC at no charge.⁹

² 41 C.F.R. § 102-81.10

³ 41 C.F.R. § 102-81.20, which requires federal agencies to adhere to minimum-security standards specified in the Department of Justice’s June 28, 1995, study entitled “*Vulnerability Assessment of Federal Facilities*” see Appendix B for “Details of Recommended Security Standards.”

⁴ 41 C.F.R. §§ 102-74.430 and 102-74.270

⁵ 41 C.F.R. § 102-74.430(f)

⁶ 41 C.F.R. § 102-74.265

⁷ 41 C.F.R. § 102-74.275

⁸ 41 C.F.R. § 102-74.305

⁹ SF 30 Modification of Contract No. FE-09-C-004, effective 10-05-09. This contract between the FEC and LAZ Parking LLC was obtained from [REDACTED] [REDACTED] in the Administrative Services Division.

The Administrative Services Division manages the assignment and use of FEC-paid parking spaces. Approximately twenty-one (21) of these FEC-paid parking spaces are designated for specific employees, positions, offices, or vehicles. The remaining eight (8) spaces are reserved for temporary (“daily”) use by employees, visitors, contractors, and/or vendors. Additionally, there are approximately 20 parking permits, which are paid for on a monthly basis, by FEC employees, to LAZ Parking.

III. SCOPE

The OIG investigated this matter from September 21, 2009, to December 29, 2009. To assess the validity of the allegations, we interviewed six FEC employees, plus [REDACTED] LAZ Parking, Ltd. [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED] was interviewed on three occasions regarding the incident on September 15th. [REDACTED], and [REDACTED] LAZ PARKING, [REDACTED] were each interviewed twice.

The staff in the Administrative Services Division was interviewed regarding the issuance of FEC-paid parking permits and Kastle keycards. [REDACTED], [REDACTED], [REDACTED] was interviewed regarding FEC policies concerning building security; parking and access controls; Kastle keycard issuance; and parking permit assignments. [REDACTED], [REDACTED] was interviewed regarding the issuance of temporary parking permits. [REDACTED], [REDACTED] was interviewed on two occasions, regarding the LAZ Parking contract and the issuance of keycards. [REDACTED], [REDACTED] was interviewed regarding the initial allegations.

The OIG gathered and reviewed agency records, which were obtained from the Administrative Services Division. These records pertained to FEC-paid parking permits and Kastle keycard access activity. The OIG reviewed procurement documents for the FEC contract with LAZ Parking Ltd; emails; parking permit assignment logs; and correspondence. The OIG reviewed relevant garage parking policies, building security access guidelines, and facilities management regulations. Additionally, the OIG collected and reviewed Kastle keycard access logs; keycard and building security policies; and applicable ethics regulations.

The case was presented to the U.S. Attorney’s Office (USAO) for review of possible criminal false statement violations under 18 U.S.C. §1001. The USAO Fraud and Public Integrity Section declined prosecution.

IV. ALLEGATIONS

The OIG investigated the following allegations:

- ❖ [REDACTED] reproduced [REDACTED] FEC-issued parking permit, so it would appear like an original permit.
- ❖ [REDACTED] allowed [REDACTED] to use [REDACTED] FEC-issued Kastle keycard, and a duplicate copy of [REDACTED] FEC parking permit, to access the garage and park [REDACTED] vehicle.
- ❖ [REDACTED] displayed a “counterfeit” FEC-paid parking permit to secure a parking space for [REDACTED] vehicle in the building garage.
- ❖ [REDACTED] accessed the FEC building garage using an FEC issued keycard assigned to [REDACTED] supervisor, [REDACTED]

The purpose of the investigation was to determine whether [REDACTED] or [REDACTED] misused government property, in violation of ethical standard, title 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property).

V. INVESTIGATION DETAILS

A. Allegations Against [REDACTED]

Allegation 1: [REDACTED] reproduced [REDACTED] FEC-issued parking permit.

The investigation determined that [REDACTED] was not authorized to reproduce or loan [REDACTED] FEC-paid parking permit to [REDACTED]. [REDACTED] admitted during OIG interviews that [REDACTED] reproduced [REDACTED] FEC-issued parking permit, using an FEC scanner and color printer. [REDACTED] began receiving FEC-paid parking benefits in June 2007, when [REDACTED] was promoted to [REDACTED]. [REDACTED] admitted that in August 2009, [REDACTED] scanned [REDACTED] original parking permit into an Adobe PDF file. [REDACTED] then printed out the image of the permit on a color printer, which was located in the main hall outside [REDACTED] FEC office. [REDACTED] then cut the image out from the sheet of paper, and attached it to a hard backing, so it would appear like a valid permit.

When questioned by the OIG, ██████ explained ██████ reason for duplicating ██████ FEC-paid permit. ██████ said ██████ wanted a “spare” permit available in ██████ “carry” bag, in case ██████ drives one of ██████ alternate vehicles to work and forgets to bring ██████ original permit. ██████ explained that ██████ keeps ██████ original permit displayed on the mirror of ██████ ██████, the vehicle ██████ normally drives to work. ██████ said ██████ has three other vehicles besides the ██████, which ██████ occasionally drives to work. ██████ wanted a duplicate “spare” parking permit kept in ██████ bag, for instances when ██████ drove an alternate vehicle to work.

During OIG interviews, ██████ further advised that a “spare” parking permit was necessary because the former head of ██████ ██████, used to conduct regular inspections of the garage, to make sure that all parked vehicles displayed a permit. According to ██████ the parking garage used to be overcrowded with vehicles and filled up quickly, due to unauthorized vehicles being parking there. ██████ felt ██████ “spare” permit would protect the parking attendant, in the event that ██████ forgets to bring ██████ original permit. By having the spare permit, ██████ could avoid the appearance that the parking attendant was allowing unauthorized vehicles to park in the garage. ██████ said ██████ “spare” parking permit should not be characterized as a “counterfeit,” since ██████ never used it for “nefarious” purposes. However, ██████ acknowledged to the OIG that ██████ was not authorized to reproduce the FEC-paid parking permit.

Allegation 2: ██████ ██████ allowed ██████ ██████ to use ██████ FEC keycard, and a duplicate copy of ██████ parking permit, to access the FEC garage and park ██████ vehicle.

The OIG investigation determined that ██████ gave ██████ permission on September 14, 2009, to use the duplicate copy of ██████ FEC-paid parking permit. ██████ told the OIG that ██████ loaned ██████ duplicate parking permit to ██████ because ██████ planned to drive into work the following day. ██████ who normally commutes to work by bus, told ██████ that ██████ planned to drive ██████ car the following day, so ██████ could stay late for a personal reason. ██████ did not plan to use ██████ parking space that next day because ██████ planned to get a ride to work. ██████ said this was the only occasion ██████ allowed anyone to use ██████ FEC-paid permit, duplicate or original, to park in the garage.

██████████ said ██████████ only intended for ██████████ to use ██████████ permit on that one day, September 15th. ██████████ further advised that ██████████ gave ██████████ the duplicate copy of ██████████ permit, instead of ██████████ original permit, because ██████████ was “too lazy” to go down to the garage and retrieve the original from ██████████ car. ██████████ said the duplicate permit was there in ██████████ office, right in ██████████ bag. ██████████ said ██████████ knew ██████████ participated in the transit subsidy benefit program.¹⁰

██████████ told the OIG that ██████████ mentioned to ██████████ of ██████████ plans to drive to work the next day (September 15th), to attend a comedy hour function, sponsored by the Hispanic Caucus, at the Warner Theatre. The event was not work related. ██████████ then offered ██████████ parking space. ██████████ told ██████████ if the parking attendant questions ██████████ ██████████ should say she’s parking in the space of the ██████████.

FEC-Paid Parking Benefits are for Work Related Purposes

During the investigation, staff in the Administrative Division advised the OIG that FEC-paid parking assignments are authorized for work related purposes, and cannot be loaned to other employees. ██████████ ██████████ ██████████ ██████████, and ██████████ ██████████ ██████████, were interviewed regarding FEC-paid parking policies and procedures. ██████████ advised that FEC-paid parking permits assigned to specific employees cannot be loaned to other employees. ██████████ further advised that employees are not allowed to duplicate or reproduce FEC-paid parking permits.

██████████ advised that FEC-paid parking spaces available in the temporary pool are for daily work-related use only. Both ██████████ and ██████████ said that employees should have a work related need to obtain an FEC-paid parking permit for the day. The assignment of these temporary day permits are approved by James WILSON, Director of Human Resources. ██████████ and Alec PALMER, Acting Staff Director, are also authorized to approve requests for temporary parking permits.

The FEC Lacks a Comprehensive Parking Policy

A review of FEC policies and procedures revealed that the FEC has not implemented a comprehensive parking policy. Four policy documents were identified concerning the authorized use or assignment of FEC parking privileges. One of these documents was a draft.

¹⁰ Under FEC Commission Directive 54, participants of the FEC transit benefit program are not allowed to receive both the transit and paid parking benefits.

The first, and most comprehensive, is a draft Commission Bulletin, dated April 8, 2002, entitled "Parking Policies and Procedures." Under this draft Commission Bulletin, the priority for assigning FEC-paid parking permits was given to "(1st) official vehicles, (2nd) executive employees; [and] (3rd) any handicapped employees; ..." This draft policy defined "Executive" as a "federal employee whose management responsibilities require preferential assignment of parking privileges." This 2002 draft Commission Bulletin stated that "Executive parking will be assigned by the Staff Director..." (Attachment No. 1) According to [REDACTED] [REDACTED] a new draft parking policy is under consideration by the Staff Director's office, but has not been finalized.

A second written policy called "FEC Issued Parking Permits" was identified, which was signed by [REDACTED] [REDACTED] on November 25, 2008. [REDACTED] advised that this policy is currently in force; however, it was not found on the FEC server. This 2008 policy, similar to the 2002 draft policy, states that FEC issued parking permits are assigned to: "Senior Level Executives," as identified by the Staff Director; "handicapped/Special Needs Employees" (physical disability required); "Special Needs," for employees on temporary disability; visitors conducting official business; and employees who require after-hours parking. (Attachment No. 2)

A third policy document entitled "FEC Building Access Guidelines," effective January 26, 2009, informed FEC employees of the following: "It is the goal of the Federal Election Commission (FEC)—or 'the Agency'—to provide a safe and secure environment for all FEC employees and government information. To that end, entry points (i.e. E Street and Loading Dock) to the FEC Headquarters building are secured by armed Officers. **Access through the parking garage is allowed only by authorized personnel with valid permits** (emphasis added)." (Attachment No. 3)

[REDACTED] advised that to comply with the "FEC Building Access Guidelines," employees who do not regularly park in the garage need to get prior authorization from the Administrative Services Division to do so. [REDACTED] said [REDACTED] sent these guidelines to all FEC employees by email.

And finally, the OIG identified a "FEC Issued Parking Permit Application," which was distributed to FEC-paid parking permit holders after the September 15th incident, in October 2009. This application stated under "Rules and Regulations: Parking permits are non-transferable. Use of the parking permit by other than the employee will result in cancellation of parking privileges." (Attachment No. 4)

No written policies were identified during the investigation, which specifically prohibited the copying, reproducing, or counterfeiting of FEC-paid parking permits. Prior to the October 2009 implementation of a revised parking permit application, there was no written policy that specifically prohibited employees from loaning, sharing, or otherwise transferring an FEC-paid parking permit to other employees.

██████████ said the parking permit application ██████████ received in October 2009 was the first time ██████████ saw anything that said parking privileges were not transferable. ██████████ was unaware of this rule when ██████████ loaned ██████████ spare permit to ██████████ on September 14th. ██████████ said this was not the rule in the past because ██████████ is aware of previous Commissioners who would let others drive to work and park with the Commissioners' permit. For example, ██████████ recalled that a former Commissioner used to give ██████████ parking pass to one of ██████████ staffers to use in the garage.

██████████ said ██████████ was aware that the FEC-paid parking permits are primarily given to executive employees, such as Commissioners and senior staff. ██████████ acknowledged that ██████████ participated in the transit subsidy benefit program. ██████████ also acknowledged there is a procedure for FEC employees to obtain temporary parking permits to the garage from the Administrative Services Division. ██████████ said ██████████ knew that the event ██████████ planned to attend was a personal event.

██████████ said ██████████ only loaned ██████████ parking permit to ██████████ on this one occasion. ██████████ said ██████████ felt it was okay to loan ██████████ permit to ██████████ because it was a past practice at the Commission by others.

Commission Bulletin 2001-10 Kastle Key Procedures

██████████ admitted that on September 14th, ██████████ loaned ██████████ ██████████ Kastle keycard with the copy of ██████████ parking permit, so ██████████ could park the next day in ██████████ assigned space. ██████████ said ██████████ knew ██████████ keycard did not grant ██████████ access to the parking garage. ██████████ said ██████████ did not think it was wrong to loan ██████████ ██████████ keycard.

██████████ was questioned regarding the written Kastle Key procedures in Commission Bulletin 2001-10, dated December 18, 2001. Specifically, ██████████ was asked if ██████████ was aware of the following section in the policy:

“TRANSFER OF INSERT-KEYS Insert-keys should not be transferred from one employee to another without prior authorization by the Kastle Key Administrator or an Alternate. Kastle Systems, Inc. will be notified of the previous and new keyholders when a transfer of insert-key is authorized.” (Attachment No. 5)

In response, ██████ said ██████ was unaware of the Commission Bulletin that prohibited the transfer of Kastle keys to other employees. ██████ said ██████ knew that FEC Bulletins are circulated, but ██████ never looked at any of the Bulletins in a shared folder, on the FEC computer server. ██████ said ██████ only looked at FEC Directives on the FEC server.

██████ ██████ and ██████ ██████ advised during an interview that they shared responsibilities, along with ██████ ██████, as the Kastle keycard Administrator. ██████ advised the “Kastle Key Procedures” in Commission Bulletin 2001-10 should be followed, but ██████ acknowledged that this policy needed to be updated. ██████ advised that employees are not allowed to give Kastle keycards to other employees. ██████ further advised that in September 2009, ██████ did not have authorization from the Administrative Services Division to give ██████ Kastle keycard to another employee.

B. Allegations Against ██████ ██████

Allegation 3: ██████ ██████ displayed a “counterfeit” FEC-paid parking permit to secure a parking space for ██████ vehicle in the building garage.

██████ ██████ admitted that ██████ displayed a “spare” copy of an FEC-paid parking permit, which belonged to ██████ supervisor, to secure a parking space in the FEC garage. ██████ statement regarding the September 15th incident was consistent with that of the LAZ Parking ██████. Furthermore, the statements provided by ██████ and ██████ were corroborated by building access keycard reports, obtained from Kastle Systems, Inc.

Keycard access records showed that on September 15, 2009, at 10:14am, ██████ entered the building garage using a keycard assigned to ██████ supervisor, ██████. The garage attendant, ██████, greeted ██████ as ██████ drove down the driveway and stopped on the ramp ██████ advised that ██████ then displayed a “fake” permit to him, which ██████ was holding in ██████ hand. ██████ said ██████ told ██████ that the permit was a fake, and ██████ then confiscated the permit.

According to ██████ ██████ tried to explain to the parking attendant that the pass belonged to ██████ supervisor, ██████ who would not be parking in the garage that day. ██████ said ██████ told ██████ that ██████ allowed ██████ to use ██████ pass. ██████ told ██████ that ██████ needed to have an original permit to park ██████ car in the garage.

Keycard access records showed that at 10:17am, ██████ entered the FEC building through the garage. According to ██████ ██████ requested a valid temporary parking permit from ██████ in the Administrative Services Division. During an interview, ██████ advised that ██████ said ██████ was working late that day, and that ██████ had allowed ██████ to park in ██████ parking space. According to ██████, ██████ said ██████ didn't have ██████ original parking pass because ██████ left ██████ pass in ██████ car. ██████ said ██████ told ██████ the garage attendant was asking ██████ for a parking pass immediately. When ██████ was asked about these statements, ██████ advised that ██████ was not trying to deceive ██████, because ██████ did work late that evening, until 6pm, which is later than ██████ normal schedule.

Keycard access records showed that ██████ returned to the garage shortly before 10:25am, and according to ██████ and ██████, ██████ presented the temporary parking pass to the garage attendant. Both ██████ and ██████ stated during interviews that ██████ then confiscated the temporary permit as well. According to ██████, the two of them had a brief argument because ██████ wanted the parking passes back, and ██████ refused to return them.

Keycard access records showed that ██████ left the parking garage for the second time at 10:25am, and entered the FEC building. ██████ said ██████ went to ██████ office and told him what happened. ██████ said ██████ was then approached by one of the FEC Commissioners, who overheard the argument and inquired about the incident. ██████ told the Commissioner that "the ██████" tried to use a fake parking pass to park ██████ vehicle.

Keycard records showed ██████ entering the FEC building from the garage at 10:59am. Both ██████ and ██████ stated that ██████ went to the garage and requested the return of "█████ duplicate parking permit, which ██████ said ██████ loaned to ██████ ██████ refused to give the pass back to ██████

FEC-Paid Parking Benefits are for Work Related Purposes

The OIG investigation determined that FEC-paid parking assignments are authorized for work related purposes. ██████ ██████ ██████, and ██████ ██████ ██████, advised that FEC-paid parking spaces available in the temporary pool are for daily work-related use only. ██████ and ██████ said that employees need a work related reason to obtain an FEC-paid parking permit for the day; and that parking permits assigned to specific employees cannot be loaned to other employees.

During an OIG interview, [REDACTED] was questioned about the *FEC Building Access Guidelines*, which state: “Access through the parking garage is allowed only by authorized personnel with valid permits.” (Attachment No. 3) [REDACTED] stated that employees who do not regularly park in the garage need prior authorization from the Administrative Services Division. According to [REDACTED] requests for temporary parking permits are to be approved by James WILSON, Director of Human Resources. [REDACTED] advised that in WILSON’s absence, Alec PALMER, or [REDACTED] are also authorized to approve parking permit requests.

[REDACTED] advised during an interview that [REDACTED] did not recall whether or not [REDACTED] read the “*FEC Building Access Guidelines*.” (Attachment No. 3) [REDACTED] acknowledged that [REDACTED] must have received the guidelines by email in July 2009, because it was sent out to all FEC employees. [REDACTED] said in [REDACTED] mind, [REDACTED] had [REDACTED] supervisor’s authorization to park in [REDACTED] spot on September 15th. [REDACTED] said in hindsight, [REDACTED] realizes [REDACTED] should have parked elsewhere. [REDACTED] said the offer was made to [REDACTED] and [REDACTED] thought that was perfect, so [REDACTED] accepted. [REDACTED] said [REDACTED] did not think at the time there was anything wrong about [REDACTED] offer to “park downstairs.”

[REDACTED] advised that at the time of the incident, [REDACTED] was unaware of the 2002 draft Commission Bulletin on parking procedures, or any facility management regulations regarding parking permits. [REDACTED] said [REDACTED] participates in the transit subsidy program, but did not see a problem with parking [REDACTED] car on the day in question. According to [REDACTED] as long as you are not parking in the garage on a daily basis, you can collect transit subsidies. [REDACTED] further advised the building practice is: “if you need to park downstairs, passes are available, even if you’re in the transit subsidy program.”

[REDACTED] admitted that in the past, [REDACTED] has parked [REDACTED] car in a private lot and paid to park whenever [REDACTED] has driven into DC. [REDACTED] said [REDACTED] parked in a garage by the Fords Theatre on two occasions before, at a cost of approximately \$20 per day. [REDACTED] said [REDACTED] didn’t pay to park on September 15th because [REDACTED] boss said [REDACTED] could use [REDACTED] pass, since [REDACTED] wasn’t driving into work that day.

[REDACTED] said that [REDACTED], [REDACTED], told [REDACTED] it has been a common practice at the FEC, for people who have parking permits, to loan the permit to those who don’t. According to [REDACTED] [REDACTED] said a former Commissioner, whose name began with a [REDACTED] allowed one of [REDACTED] staff members to park in the Commissioner’s assigned space for almost 20 years. [REDACTED] said when [REDACTED] boss offered [REDACTED] the permit for September 15th, [REDACTED] said thank you and didn’t think it was unauthorized.

The investigation revealed that [REDACTED] knew the reproduced copy of the permit [REDACTED] received from [REDACTED] was not an original. [REDACTED] said that when [REDACTED] gave [REDACTED] parking permit, [REDACTED] noticed it looked funny and asked him, "what's this?" According to [REDACTED] [REDACTED] explained it was a spare pass for the downstairs garage, which [REDACTED] kept in case [REDACTED] doesn't have [REDACTED] parking pass. [REDACTED] also stated to the OIG that it was obvious the duplicate pass [REDACTED] gave [REDACTED] was only a copy, and [REDACTED] told [REDACTED] that this was "what I use for my other cars."

[REDACTED] believed [REDACTED] was authorized to receive FEC-paid parking benefits that day because [REDACTED] supervisor, [REDACTED] gave [REDACTED] permission to park in the garage. [REDACTED] said that since [REDACTED] was authorized to park [REDACTED] vehicle in the garage, and was not planning to park that day, [REDACTED] believed it was appropriate for him to allow [REDACTED] to park there.

Allegation 4: [REDACTED] accessed the FEC building garage using an FEC issued keycard assigned to [REDACTED] supervisor, [REDACTED]

Kastle keycard access records indicated that on September 15, 2009, at 10:14am, [REDACTED] entered the building garage using a keycard assigned to [REDACTED] supervisor, [REDACTED]. [REDACTED] advised that [REDACTED] gave [REDACTED] keycard to [REDACTED] with the duplicate parking permit, because [REDACTED] knew that [REDACTED] keycard would not allow [REDACTED] access to the garage.

When initially questioned by the OIG, [REDACTED] claimed that [REDACTED] used [REDACTED] own Kastle keycard to access the garage. [REDACTED] initially denied receiving a keycard from [REDACTED] supervisor [REDACTED]. During a second interview, when confronted with keycard access records, [REDACTED] acknowledged that [REDACTED] reminded [REDACTED] that [REDACTED] let [REDACTED] use [REDACTED] keycard to access the garage on September 15th. [REDACTED] said [REDACTED] still could not recall that [REDACTED] received a keycard from [REDACTED] or that [REDACTED] used [REDACTED] keycard on September 15th, or that [REDACTED] returned [REDACTED] keycard to him after the incident. However, [REDACTED] did not dispute the fact that these incidents occurred.

During an OIG interview, [REDACTED] was shown the written Kastle Key procedures in Commission Bulletin 2001-10, dated December 18, 2001. Specifically, [REDACTED] was asked if [REDACTED] was aware of the following section in the policy:

"TRANSFER OF INSERT-KEYS Insert-keys should not be transferred from one employee to another without prior authorization by the Kastle Key Administrator or an Alternate. Kastle Systems, Inc. will be notified of the previous and new keyholders when a transfer of insert-key is authorized."(Attachment No. 5)

In response, ██████ said ██████ was unaware that this Commission Bulletin was saved on the FEC-wide server. ██████ was unaware that the FEC had a Kastle key procedure bulletin. ██████ said it makes sense that authorization is required when a keycard is transferred long term, to know who is coming in and out of the building. ██████ said ██████ felt that a loan of a Kastle key for a day was okay.

As previously stated under allegation 2 above, ██████ ██████ and ██████ ██████ were interviewed regarding Kastle keycard procedures. ██████ said the “Kastle Key Procedures” in Commission Bulletin 2001-10 should be followed, but the policy needed to be updated. ██████ said that employees are not allowed to give Kastle keycards to other employees; and that ██████ did not have authorization from the Administrative Services Division to give ██████ keycard to another employee in September 2009.

VI. FINDINGS

As to ██████ ██████

Our investigation concluded that ██████ misused ██████ government issued FEC-paid parking permit, and ██████ Kastle keycard, in violation of the ethics regulation, 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). The OIG found that ██████ improperly reproduced ██████ FEC-paid parking permit, in light of federal parking regulations and FEC building access guidelines, which require a valid permit for garage access. ██████ acknowledged that ██████ did not have permission or authorization to duplicate ██████ FEC-paid permit.

Our investigation found that ██████ made improper use of FEC resources, and acted improperly, by allowing ██████ to use ██████ government assigned property (executive parking privileges and keycard). The OIG found that on one occasion, ██████ allowed ██████ to use ██████ FEC issued keycard and duplicate parking permit, so ██████ could access the garage and park ██████ car for free. We found that ██████ purpose for parking in the garage on September 15th was unrelated to ██████ job, so ██████ could attend an after-work comedy event at the Warner Theatre. We also found that Commission Bulletin 2001-10, which requires prior authorization to transfer Kastle keycards from one employee to another, was available for ██████ to review, in a shared folder on the FEC server.

As to [REDACTED] [REDACTED]

Our investigation substantiated the allegations made against [REDACTED]. The OIG concluded that [REDACTED] displayed a copy of an FEC-paid parking permit, made to look like a real permit, so [REDACTED] could secure a parking space in the building garage. We further found that [REDACTED] used [REDACTED] supervisor's keycard to gain street access to the building garage. However, we concluded that these acts did not constitute administrative misconduct, in violation of the ethics regulation, 5 C.F.R. § 2635.704 (Unauthorized Use of Government Property). We concluded that [REDACTED] supervisor improperly authorized [REDACTED] use of both [REDACTED] duplicate parking permit, and [REDACTED] Kastle keycard.

The OIG also based our conclusion on the fact that at the time of the incident, the FEC did not have clear policies in place, governing the proper use of parking permits and keycards. The investigation found that the FEC lacks a clear and widely disseminated directive or policy, which prohibits the loaning or temporary transfer of Kastle keycards from one employee to another.

Although we did not conclude any misconduct by [REDACTED] we believe [REDACTED] exercised poor judgment in presenting a duplicate copy of [REDACTED] supervisor's parking permit, to park [REDACTED] vehicle in the garage. Our investigation found that [REDACTED] knew [REDACTED] did not receive [REDACTED] original permit. We were also troubled by the fact that [REDACTED] used the duplicate permit to obtain FEC-paid parking benefits, so [REDACTED] could attend a personal comedy hour event that evening at the Warner Theater. [REDACTED] was a recipient of transit subsidy benefits, and acknowledged that [REDACTED] was not eligible to receive executive parking privileges.

VII. RECOMMENDATIONS

- ❖ Because [REDACTED] [REDACTED] has plans to retire in January 2010, we make no recommendations regarding [REDACTED] actions.
- ❖ Because we found no administrative misconduct, only poor judgment, by [REDACTED] [REDACTED] we recommend counseling for [REDACTED] regarding proper use of parking permits and keycards.
- ❖ To ensure compliance with the goals and objectives of federal regulations and security standards, we recommend the FEC implement and widely disseminate a clear and comprehensive policy to govern the assignment and utilization of parking spaces at the FEC building. A proposed parking policy should establish procedures for permit

applications; vehicle updating requirements; permit display requirements; temporary permit justifications; priority of assignments; permit transfer restrictions; and prohibitions on falsifying, forging, counterfeiting, altering, or reproducing permits, or permit applications. A proposed parking policy should also provide for the loss of parking privileges, and other consequences, if the procedures are violated. We also recommend that the garage parking attendant be provided a list of vehicles and drivers authorized to park in the FEC garage.

- ❖ To enhance security measures and building access controls, we recommend the FEC implement and widely disseminate clear procedures to place accountability over the issuance, use, inventory, and deactivation of Kastle Systems keycards. Procedures should specifically prohibit the sharing, transfer, or unauthorized use of keycards. A process should be implemented to ensure that all active keycard users are accurately identified. This policy should also have a lost or stolen reporting requirement, to ensure prompt keycard deactivation.

VIII. PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENT LIST

Attachments #	Description
1	Draft Commission Bulletin 2002- : <u>Parking Policies and Procedures</u> , dated April 8, 2002.
2	<u>FEC Issued Parking Permits</u> : FEC policy and procedures signed by [REDACTED] on November 25, 2008.
3	<u>FEC Building Access Guidelines</u> : issued by the Office of the Deputy Staff Director, effective January 26, 2009.
4	<u>FEC Issued Parking Permit Application</u> , signed by [REDACTED] [REDACTED] on December 23, 2009.
5	Commission Bulletin 2001-10: <u>Kastle Key Procedures</u> , dated December 18, 2001.

Attachment No. 1

Draft Commission Bulletin 2002-:
Parking Policies and Procedures
dated April 8, 2002.

Case Number INV-10-01

Commission Bulletin 2002 -

April 8, 2002

TO: Commissioners
Commission Staff

FROM: Sylvia E. Butler
Administrative Officer

SUBJECT: Parking Policies and Procedures

1. **PURPOSE.** The purpose of this bulletin is to establish and implement policy, procedures, priorities, and criteria for the use and assignment of parking spaces.
2. **EXCLUSIONS.** An employee who has an FEC parking permit is not entitled to receive the transit subsidy. Individuals with long-term temporary (i.e. 30 days or longer) parking permits based on medical documentation are also not eligible to receive the transit subsidy while they hold the temporary permit.
3. **DEFINITIONS.**
 - a. **Official Vehicle.** A government-owned or leased vehicle used for official purposes.
 - b. **Physically-challenged employee.** An FEC employee who has permanent or temporary physical disability as supported by appropriate medical documentation and approved by FEC management.
 - c. **Executive.** A federal employee whose management responsibilities require preferential assignment of parking privileges.
 - d. **Car/Van Pool.** A group of two or more federal employees, all of which must be FEC employees, who work full-time, 4 days or more per week, using a motor vehicle for transportation to and from work on a continuing basis.
 - e. **After-Hours Parking.** The time after the official close of business up until the beginning of the next business day. This shall include after 5:30 p.m. on any work day (Monday through Friday); any time on the weekend; and holidays.

4. **POLICY and PROCEDURE**. It is the policy that FEC-paid parking permits will be assigned to FEC employees, in the priority order that follows: (1st) official vehicles; (2nd) executive employees; (3rd) any handicapped employees; (4th) vendors/visitors; (5th) union car/van pools; (6th) non-bargaining unit car pools and (7) individuals. The Union is allowed one (1) parking space for a car/van pool. At least two (2) parking spaces are normally set aside for physically challenged employees.
- a. **Individual Parking Spaces**. Parking spaces for individual employees (bargaining or non-bargaining) will be offered when available but not paid for by FEC.
- b. **Physically-challenged Employees**. Physically-challenged employees requesting temporary or permanent parking must submit a letter from a licensed physician. Parking for physically-challenged employees is not transferable and may only be utilized by the parking permit holder. Requests for permanent or temporary permits must be approved by the Deputy Staff Director.
- c. **Executive**. Executive parking will be assigned by the Staff Director and Deputy Staff Director, in his/her absence.
- d. **After-Hour Parking**. Written requests for parking after hours to conduct official business must be approved by the Division/Office Head and submitted to the Administrative Officer at least one day prior to the date needed. If a permit is available, a parking permit will be issued on a temporary basis. The permit must be returned to the Administration Division the next working day after its use. Permit holders must have an authorized kastle key with garage access in order to enter the parking garage after hours.
- e. **Visitors/Vendor Parking**. Written requests for parking permits to be used by visitors and/or vendors conducting official business during the work day must be submitted from the Division/Office Head directly to the Administrative Officer at least one day prior to the date needed. The written request must include: 1) visitor's name; 2) date and time of visit; 3) purpose of visit; 4) color, make, model of car and 5) issuing state and tag number of the vehicle. If a permit is available, Administration will issue a parking permit on a temporary basis.

5. **SECURITY**

- a. All employees who park in the garage and leave after 6:00PM, Monday thru Friday, may pick up their keys from the lobby guard's desk. The parking garage attendant will deliver the keys to the lobby guard's desk and place them in a wooden file box. The security guards are not responsible for safeguarding any keys left at their desk.
- b. All employees are responsible for maintaining their assigned parking permit and garage key card in a secured area.

6. **PERMANENT PARKING PERMIT ALLOCATION**

- a. If an FEC employee relinquishes his/her individually paid for parking space, they must report the vacancy to MetroPark on (703) 433-0582 and the Administration Division on x1240. Vacant parking spaces not returned by FEC for purpose outlined in #4 will be offered first based on the priorities set forth in Section 4 above. If no FEC employee requests the parking space, FEC will pay for the space until it can be filled.

Questions concerning this bulletin should be directed to Admin. on x1240.

Attachment No. 2

FEC Issued Parking Permits

FEC policy and procedures signed by Aileen BAKER
on November 25, 2008.

Case Number INV-10-01

FEC ISSUED PARKING PERMITS

Policy and Procedures: It is the policy of the FEC that all FEC issued parking permit holders certify eligibility and compliance for use and assignment of parking spaces in the garage.

It is the policy of the FEC that parking permits be assigned to the following groups:

Senior Level Executives as identified by the Staff Director.

Handicapped /Special Needs Employees An FEC employee who has a physical disability that presents a significant hardship in the use of public transportation. Medical documentation will be required for issuance of a permit due to disability.

Special Needs Request for parking for employees on temporary disability, request for parking for visitors conducting official business during work and request for parking for employees who require After-Hours Parking.

OHR will verify that employees issued Permanate or Handicapped parking permits do not participate in the Transit Subsidy Program at the FEC.

Signature



Administrative Services Manager

Date

11-25-08

Attachment No. 3

FEC Building Access Guidelines:
issued by the Office of the Deputy Staff Director,
effective January 26, 2009.

Case Number INV-10-01

FEC BUILDING ACCESS GUIDELINES

(Effective January 26, 2009)

Homeland Security Presidential Directive-12 (HSPD-12) mandates the development and implementation of a government-wide standard for a secure and reliable new identification card issued to Federal employees and contractors. The overall goal of HSPD-12 is to achieve appropriate security assurance by verifying the identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems. It is the goal of the Federal Election Commission (FEC)—or 'the Agency'—to provide a safe and secure environment for all FEC employees and government information. To that end, entry points (i.e. E Street and Loading Dock) to the FEC Headquarters building are secured by armed Officers. Access through the parking garage is allowed only by authorized personnel with valid permits.

The Agency issues HSPD-12 PIV badges to Federal personnel, approved contractors and other eligible individuals. FEC employees and contractors with current Personal Identity Verification (PIV) badges gain access by properly displaying their badge to the Security Officer. Access will be granted only through the E Street entrance. Access through the parking garage is allowed only by authorized personnel with valid permits. A visitor—who is considered to be any individual without a FEC issued badge—may obtain access by signing in and being escorted by a FEC employee.

All PIV badges are the property of the FEC and are to be used for official purposes only. The Agency reserves the right not to issue a card or to require the surrender of a previously issued card. Individuals receiving PIV badges agree to abide by the FEC policy concerning these badges. **ANY INDIVIDUAL FAILING TO COMPLY WITH THESE MANDATORY ACCESS PROCEDURES WILL NOT BE GRANTED ADMITTANCE TO THE BUILDING.**

Admittance of Employees and Contractors

FEC employees and contractors must display a valid FEC issued PIV badge to the Security Officer to be admitted into FEC controlled space. If, for any reason, you do not have your badge, you must sign-in with the Security Officer at the front desk. The Security Officer will confirm your employment and then issue you a one-day Visitor badge, which must be returned upon your departure from the building. **NOTE: It is mandatory that employees and contractors carry their PIV badge at all times while in FEC facilities.**

Temporary Employees and Contractors

Employed greater than 6 months:

All temporary employees and contractors who will require building access for more than six (6) months are subject to the PIV badge procedures applicable for permanent employees.

Employed 6 months or less:

- Administrative Services Division will provide temporary employees and contractors with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems;
- Identity credentials issued to these individuals will be visually and electronically distinguishable from identity credentials issued to permanent staff; and
- Managers and supervisors must apply adequate controls to systems and facilities (i.e. ensuring temporary staff has limited/controlled access to facilities and information systems);

Visitor Access Procedures

FEC offices that sponsor seminars, meetings, working groups, etc. can help speed the visitor access process by providing the Administrative Services Division (ASD) with as much advance notice as possible. ASD will ensure the Security Officer(s) have the information for processing FEC visitors. Without advance notification, Security Officers **must** contact a FEC employee to verify the official nature of the visit and/or sponsor the individual entering the FEC facility.

In order to provide minimum delays for visitors, please email the Administrative Services Division (*AdministrativeServicesDivision@fec.gov*). The e-mail should contain the name of the visitor, date, approximate time and sponsor's name and number or call (202-694-1240) when immediate attention is needed. Last minute notifications can cause delays. Please inform your visitors that they must show the Security Officer a valid picture ID (drivers license, military ID, etc.). They will be required to sign-in at the building security desk, process through the walk-through magnetometer, have their items x-rayed or searched and be escorted while in the building.

Lost/Stolen ID Badges

Employees and contractors must report lost/stolen PIV Badges to Administrative Services Division as soon as you become aware of the loss. Transportation to the vendor (i.e. ORC) providing the FEC ID Cards will be provided by the Administrative Services Division on a bi-monthly basis or as scheduled. Temporary ID badges will not be issued. Employees or contractors without a valid PIV badge will have to access the building under the visitor access procedures, except that employees will not need a sponsor. Once issued, PIV badges are the responsibility of the individual. Multiple lost, stolen or damaged badges through negligence (i.e. determined on a case-by-case basis) will be replaced at the individual's expense.

Damaged Badges

Bring damaged badges to Administrative Services Division for replacement. If a damaged badge has not expired and the badge can be authenticated, ASD will schedule a time with ORC at their facility to have a new badge issued. This will be on the same bi-monthly schedule as new employees and replacement badges will be issued. The expiration date on the new badge will be the same as the date on your broken badge. Once issued, PIV badges are the responsibility of the individual. Multiple lost, stolen or damaged badges through negligence (i.e. determined on a case-by-case basis) will be replaced at the individual's expense.

Invalid or Former Badges

Individuals possessing invalid or old FEC issued badges must turn them in to ASD. Security Officers are authorized to and will confiscate all FEC issued PIV badges that are invalid (e.g. expired date) and any formerly FEC issued non-PIV badges.

Government Property

Capitalized government property (e.g. laptops, furniture, etc.) must be cleared by the Security Officer(s) in order to remove it from the building.

Attachment No. 4

FEC Issued Parking Permit Application
signed by [REDACTED] on December 23, 2009.

Case Number INV-10-01



FEC ISSUED PARKING PERMIT APPLICATION

Please complete and sign the application form below. Please also make sure that you read the *Parking Rules and Regulations* listed below.

EMPLOYEE INFORMATION

DATE: 12-11-09

NAME: [REDACTED] Ext # [REDACTED] DEPARTMENT [REDACTED]

Vehicle Information [REDACTED] Year, Make, Model, Color [REDACTED] License Plate [REDACTED] State VA

Rules and Regulations:

- ❖ Parking permits are non-transferable. Use of the parking permit by other than the employee will result in cancellation of parking privileges.???
- ❖ **Special Needs:** Request for parking for employees on temporary disability requires medical documentation stating period of time permit will be required; request for parking for visitors conducting official business during work and request for parking for employees who require After-Hours Parking.
- ❖ All employees must also certify that they do not participate in the Transit Subsidy Program at the FEC.
- ❖ Do you currently participate in a car/van pool? Yes ___ No
If you answered "Yes" please provide the names of those participating in your car/van pool.

Name/s: 1. _____ 2. _____ 3. _____

Employee Signature [REDACTED] Date 12-23-09

Attachment No. 5

Commission Bulletin 2001-10: Kastle Key Procedures
dated December 18, 2001.

Case Number INV-10-01

December 18, 2001

Commission Bulletin 2001 - 10
Supersedes Commission
Directive no. 55 dated June 15, 1992

TO: Commissioners
Commission Staff

FROM: Sylvia E. Butler
Administrative Officer

SUBJECT: Kastle Key Procedures

The Administration Division has implemented these procedures in order to control the assignment of new insert-keys and to maintain the proper records of lost, broken or stolen insert-keys.

Kastle Systems, Inc. provides an Access Control System for the 999 E Street Building which requires authorized employees to utilize an insert-key to enter the building and access the elevators during non-work hours and to enter the garage 24 hours/7 day a week. The front door to the building and the elevators will be locked from 6:00 PM to 6:30 AM, Monday through Friday, and 24 hours a day on weekends and holidays. The elevator and stairwell entrances from the garage are locked at all times and only parking permit holders can access the building from the garage using an insert-key. The Access Control System records the time, date, insert-key number and the name of the employee who gained entry to the building, elevators or garage during non-work hours. Instructions for the Insert-Key Access Control System are attached.

ASSIGNMENT OF PERMANENT AND TEMPORARY INSERT-KEYS

Division and Office Heads who wish to have their staff members receive a permanent or temporary insert-key should send the Administration Division an email or memorandum with the name of the person who is to receive the insert-key. The employee will be notified by Patricia Dunn, the Kastle Key Administrator when the insert-key is ready for pick-up. When a permanent insert-key is assigned, the employee will be required to sign a Kastle Key receipt form acknowledging that the insert-key was received. For use of a temporary insert-key, the employee must sign the Kastle Insert-key Temporary Use Log acknowledging that the insert-key was received and the date when the key is to be returned. The employee must sign the log again when the insert-key is returned.

LOST, BROKEN AND STOLEN INSERT-KEYS

Employees should report lost, broken and stolen insert-keys to the Kastle Key Administrator who will notify Kastle Systems, Inc., of the key number and request that the key be revoked from access to the system immediately. If the key is broken, the employee should return the insert-key to the Kastle Key Administrator for disposition.

TRANSFER OF INSERT-KEYS

Insert-keys should not be transferred from one employee to another without prior authorization by the Kastle Key Administrator or an Alternate. Kastle Systems, Inc. will be notified of the previous and new keyholders when a transfer of insert-key is authorized.

EMPLOYEES LEAVING THE AGENCY

If an employee leaves the agency, the insert-key must be returned to the Kastle Key Administrator. Kastle Systems will be notified that the employee has left the agency and the insert-key will be revoked until it is reassigned to another employee. If an employee leaves the agency without turning in his/her insert-key, it will be immediately revoked from having access to the system. The Personnel Office will ensure that all employees leaving the agency report to the Administration Division during the exit clearance process which will include clearance by the Kastle Key Administrator.

If there are any questions concerning these procedures, please call Patricia Dunn or Sylvia Butler on 694-1240.

Attachment

Attachment 1

INSTRUCTION FOR OPERATION OF THE KASTLE INSERT-KEY ACCESS CONTROL SYSTEM

The Kastle Insert-Key Access Control System deters unauthorized entry, while allowing tenants and their visitors easy access to the building when it is locked. Tenants are to use the insert-keys in the readers installed at 1) the front door; 2) garage door; 3) stairwell; 4) and elevator doors in the lower level.

BUILDING ENTRY

Insert the insert-key into the reader and remove it immediately. If the insert-key is authorized, the flashing light on the reader will glow continuously, and the door will unlock. If the door does not unlock, try again. If after two attempts the door does not unlock, you may call the hotline number (703) 524-7911 and give the Monitor Center operator your name and/or key number. The operator will verify that you have an authorized key and will give you access into the building.

If an FEC employee needs to enter the building during non-work hours, but does not have a insert-key, Kastle Systems will consider the employee a visitor and he/she must call the Kastle Systems hotline number on (703) 524-9411 to request access into the building. The hotline operator will request the employee's name and the telephone number of the office the visiting employee will be working in. The Kastle System Operator will contact the Administrative Officer or Kastle Key Administrator to obtain authorization for allowing an employee to enter building.

ELEVATOR ENTRY

Board the elevator and insert your insert-key into the reader. When the red light on the reader glows continuously, press the floor button. FEC employees' insert-keys are only authorized to allow elevator access to the 2nd, 4th, 6th, 7th, 8th and 9th floors during non-working hours.

BUILDING/ELEVATOR EXIT

You may exit from the building via the elevators, without using the insert-key and the elevators will take you to the Lobby floor.

GARAGE ENTRY

An employee with a parking permit in the garage is authorized to have garage access activated on the kastle insert-key. All permit holders will need their insert-key to enter the elevator lobby and stairwell door from the garage.



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CASE CLOSING MEMORANDUM

Case #: INV-10-02	Prepared By: J. C. THURBER
Case Title: [REDACTED]	
Date of Report: March 14, 2011	
Subject: Computer Breach	

Hotline Complaint HL-10-09 was opened on May 5, 2010, when the Office of Inspector General (OIG) received a Hotline complaint from [REDACTED], [REDACTED] of [REDACTED], that he had been receiving anonymous calls to his cellular telephone concerning [REDACTED] relationship with [REDACTED] and that [REDACTED] FEC email account might have been hacked. Interviews were conducted and computer analyses were performed. Based on this information, an investigation was opened on June 14, 2010.

[REDACTED] believed [REDACTED] email had been breached because [REDACTED] had allegedly received through the U. S. Mail a printed email (April email) from [REDACTED] to another FEC employee. Computer analysis revealed that there had been no email account breach from the outside, and the April email had been sent from [REDACTED]'s FEC-issued Blackberry to an email account exclusively controlled by [REDACTED]. Only [REDACTED], [REDACTED] and [REDACTED] had access to the Blackberry when the April email was forwarded. [REDACTED] refused to provide cellular telephone records that would have substantiated [REDACTED] allegation of anonymous calls, and [REDACTED] eventually stopped cooperating with the investigation. Based on this evidence, it appeared that [REDACTED] may have improperly accessed the FEC email system through [REDACTED] FEC-issued Blackberry. DOJ declined prosecution.

OIG Disposition:

The OIG issued a Report of Investigation to the Commission and FEC management on February 24, 2011. In the report, the OIG recommended that management clarify its policies related to reporting attempted security breaches and to increase training in that area. No further investigative activity is required. Therefore, this investigation is closed.

Concurrence: _____

Jon Hatfield, Deputy Inspector General

_____ Date

**FEDERAL ELECTION COMMISSION
OFFICE OF INSPECTOR GENERAL**



Report of Investigation

■■■■■■■■■■ ■■■■■■■■■■
Case Number INV-10-02

February 24, 2011

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

<u>Table of Contents</u>		<u>Page</u>
I.	Executive Summary	1
II.	Allegation	2
	An unidentified person repeatedly and anonymously contacted [REDACTED] by telephone and someone improperly accessed [REDACTED]'s FEC email account.	
III.	Background	3
	A. Relevant Statutes, Regulations and Policies	3
	B. Scope of the Investigation	3
IV.	Investigation Details	4
	A. Anonymous Telephone Calls	5
	B. Computer Breach Involving April Email	7
	C. Previous Attempts to Access [REDACTED] Electronic Communications	10
	D. Relevant Computer Security Training	11
V.	Findings	12
VI.	Recommendations	13
VII.	Privacy Act and Freedom of Information Act Notice	14
	Attachment List	15

I. Executive Summary

On May 5, 2010, the Office of Inspector General (OIG) received a hotline complaint via email from [REDACTED] ([REDACTED] the [REDACTED] of [REDACTED] ([REDACTED] for the Federal Election Commission (FEC) [REDACTED]. [REDACTED] alleged that [REDACTED] had been repeatedly and anonymously contacted by telephone about an alleged relationship between [REDACTED] and [REDACTED],¹ and that the calls usually came around the times of [REDACTED] or when “they are in private meetings together.” [REDACTED] was unable to provide any information concerning the dates and times of the anonymous calls [REDACTED] claimed to have received, and eventually stopped cooperating with the investigation. [REDACTED] further alleged that [REDACTED] FEC email account might have been improperly accessed.

During [REDACTED] interview, [REDACTED] claimed that in addition to receiving anonymous telephone calls over an approximately eight month period warning of [REDACTED] alleged relationship with [REDACTED], [REDACTED] also had received through the United States Mail an anonymously sent “letter.” This “letter” was later identified as an email sent between [REDACTED] and [REDACTED] FEC email accounts on April 1, 2010, which had been printed out (April email). The April email described [REDACTED] feelings about [REDACTED]. [REDACTED] were interviewed.

The investigation determined that the April email was originally sent electronically from [REDACTED] FEC email account to [REDACTED] FEC email account on Thursday, April 1, 2010, at 6:31 p.m., there were no other recipients, and [REDACTED] and [REDACTED] claimed to have not printed or otherwise provided the email to anyone. Because [REDACTED] alleged to have received the April 1 email, the [REDACTED] and [REDACTED] suggested to the OIG that a possible computer breach occurred. Because of the possible breach of the FEC email system, [REDACTED] and [REDACTED] FEC-issued Blackberry personal communication devices (PCDs), netbooks and laptop computers were turned over to the OIG and analyzed. [REDACTED] and [REDACTED] Lotus Notes government accounts, of which their FEC email accounts are a part, were also analyzed. The Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS) was consulted for technical and legal advice.

The computer analyses revealed that [REDACTED] and [REDACTED] were the only ones with access to the email programs of their respective FEC accounts, and it did not appear that either account had been broken in to. The investigation revealed that on Sunday, April 4, 2010, at 1:24

¹ [REDACTED] is not pertinent to the alleged violations and the OIG found no evidence rising to a level to pursue an investigation into whether the relationship between [REDACTED] and [REDACTED].

p.m., the April email was forwarded electronically from ██████████ FEC email account sent folder via ██████████ FEC-issued PCD, which ██████████ usually keeps in the ██████████ of ██████████ on weekends, to an email account exclusively controlled by ██████████ Only ██████████ ██████████ and ██████████ had access to ██████████ FEC-issued PCD at the time the April email was forwarded. It was discovered that ██████████ admitted to either accessing or attempting to access ██████████ electronic communications on three prior occasions, including a previous attempt to access ██████████ FEC-issued PCD sometime between October 2009 and January 2010. ██████████ did not report this previous attempted breach to the ITD Help Desk and did not take additional steps to secure ██████████ FEC-issued PCD at ██████████ residence.

DOJ declined to prosecute any criminal violation related to this matter. Based on these findings and a review of FEC Information System Security Program Policies 58A and 58-4.4, and Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and Systems Resources (Rules of Behavior), the OIG recommends revising the policies and Rules of Behavior to explicitly require that attempted security breaches be reported. The OIG further recommends providing general and PCD security training and copies of ITD security policies each and every time a PCD is issued to a FEC employee or contractor.² Management should consider whether any action is necessary in regards to ██████████ for failing to report a security problem or incident, and for not adequately securing ██████████ FEC-issued PCD.

II. Allegation

The OIG investigated ██████████ allegation that an unidentified person repeatedly and anonymously contacted ██████████ by telephone about an alleged relationship between ██████████ and ██████████, and improperly accessed ██████████ FEC email account. Evidence obtained during the investigation suggests that ██████████ may have improperly accessed ██████████ FEC email account and provided false information to the OIG about how ██████████ came to be in possession of the April email. ██████████ eventually ceased cooperating in the investigation. As a result, the OIG was unable to substantiate ██████████ allegation concerning the anonymous telephone calls, as ██████████ is the only known witness with direct knowledge of the calls.

² The final report of the OIG's Audit of the Commission's Property Management Controls, audit assignment OIG-09-02, issued March 2010, pg. 24, recommended that PCD policies and procedures should be provided to all PCD users upon issuance of a PCD. Management responded that "[a]ll users will be directed to [a shared folder accessible to all FEC personnel] so they may review applicable directives."

III. Background

A. Relevant Statutes, Regulations and Policies

It is a crime under 18 U.S.C. § 1030(a)(2)(C) for anyone to “intentionally access[] a computer without authorization or exceed[] authorized access” and obtain “information from any protected computer.” The definition of “computer” includes PCDs, and United States Government computers are “protected computers.” 18 U.S.C. §§ 1030(e)(1), (2)(A). FEC-issued PCDs are United States Government computers, and therefore “protected computers.” 18 U.S.C. § 1030(e)(2)(A).

Anyone who knowingly and willfully falsifies or conceals a material fact or makes any materially false, fictitious, or fraudulent statement or representation in any matter within the jurisdiction of the United States Government commits a crime under 18 U.S.C. §§ 1001(a)(1) and (2). False or misleading statements made during the course of an OIG investigation that may potentially lead the investigation off track are material and may comprise a violation of the statute. U. S. v. Silva, 119 Fed. Appx. 892 (9th Cir. 2004).

It is an administrative violation of 5 C.F.R. § 2635.704 to use government property, including telephones, computers and communications devices, for other than authorized purposes. Federal Election Commission Directive 58 § C states that *de minimis* personal use of FEC telephones and the FEC computer system is allowed, as long as the use is “appropriate.” The term “appropriate” is not further explicitly defined or explained.

FEC Information System Security Program Policy 58A §§ 2.c and 4.a.i state that employees have personal responsibility for safeguarding and protecting all FEC electronic information. Further, § 4.a.iii states that employees must notify the FEC Help Desk whenever a “security problem” is discovered. The term “security problem” is not further defined or explained. According to FEC Personal Communication Devices Security Policy 58-4.4, § 2.k, “Any FEC-issued PCD must be secured at all times.”

FEC Rule of Behavior number 17 requires employees to protect “FEC computing resources from theft or loss,” and to “take particular care to protect any portable devices” such as FEC-issued PCDs. Rule of Behavior number 22 requires employees to “[p]romptly report all security incidents in accordance with FEC policy.” As with the term “security problem,” the term “security incident” is not further defined or explained, and the terminology is inconsistent with FEC Information System Security Program Policy 58A § 4.a.iii.

B. Scope of the Investigation

The OIG began a preliminary inquiry of this matter on May 5, 2010, and Hotline complaint number HL-10-09 was assigned. The formal investigation was opened on June 14, 2010. The OIG

interviewed [REDACTED] and [REDACTED] was interviewed by telephone. [REDACTED] was interviewed three times, once with [REDACTED] present at [REDACTED] request, and twice alone. The OIG attempted to re-interview [REDACTED] in person, but [REDACTED] declined to cooperate further.

The FEC turned over to the OIG and we conducted analyses of [REDACTED] and [REDACTED] FEC-issued computers, netbooks and PCDs. The OIG consulted with the FEC's Enforcement Division and an [REDACTED], who helped perform the computer analyses on behalf of the OIG. [REDACTED] and a [REDACTED] conducted analyses of the FEC email accounts of [REDACTED] and [REDACTED] the original respective sender and recipient of the April email. In addition, the OIG reviewed outgoing FEC long distance telephone records obtained from the Administrative Services Division in an attempt to determine if any calls had been placed to [REDACTED] cellular telephone from an FEC telephone line, other than that of [REDACTED] FEC ITD computer security training records were also reviewed.

IV. Investigation Details

This matter was initiated on May 5, 2010, when [REDACTED] emailed a Hotline complaint to the OIG at 8:53 a.m., stating that [REDACTED] had been repeatedly and anonymously contacted by telephone about a relationship between [REDACTED] and [REDACTED]. (Attachment 1) [REDACTED] stated that the calls usually came around the times of [REDACTED] or when "they are in private meetings together." *Id.* [REDACTED] further claimed that [REDACTED] FEC email account might have been improperly accessed, and that [REDACTED] was planning to meet with ITD later that day.

[REDACTED] met with the OIG on May 5, 2010 to discuss the incident, and [REDACTED] was also present at [REDACTED] request. At this meeting, [REDACTED] first mentioned the April email, which [REDACTED] believed [REDACTED] had received the previous week through the United States Mail. [REDACTED] was interviewed by telephone on May 6, 2010, the day after [REDACTED] made the complaint.

Joe SPRINGSTEEN, a DOJ attorney at CCIPS, was consulted and briefed on the facts of the investigation. On July 12, 2010, SPRINGSTEEN, who is also a Special Assistant United States Attorney for the District of Columbia, informed the OIG that the DOJ was issuing a declination of prosecution in this matter.

A. Anonymous Telephone Calls

The primary concern indicated by [REDACTED] in [REDACTED] initial email of May 5, 2010, was that [REDACTED] had repeatedly received anonymous calls about the alleged relationship between [REDACTED] [REDACTED] [REDACTED] and [REDACTED]. [REDACTED] stated in [REDACTED] email, "The nature of this contact is to apparently alert me about the nature of their relationship and they expressed that it is more than professional." [REDACTED] continued that [REDACTED] tried but was unable to determine the origin of the calls, which "happened around [REDACTED] and when they are in private meetings together."

On May 6, 2010, OIG personnel interviewed [REDACTED] and [REDACTED] stated the following:

- [REDACTED] received three anonymous calls to [REDACTED] cellular telephone from a female warning about [REDACTED] wife's relationship with [REDACTED]. The first anonymous call was in October 2009, the second "[REDACTED] [REDACTED]," and the third call was in 2010.
- The caller ID on [REDACTED] cellular telephone displayed "Unknown" for all the calls. The caller may have obtained [REDACTED] cellular telephone number from [REDACTED].
- [REDACTED] received other calls late at night, but nothing was said.

[REDACTED] was interviewed on May 6, May 11, and August 9, 2010, about the anonymous telephone calls, and other matters related to the case. While [REDACTED] is the only person with direct, first-hand knowledge of the calls, [REDACTED] discussed them with [REDACTED] [REDACTED] stated the following:

- [REDACTED] is aware of three anonymous calls placed during the day to [REDACTED] [REDACTED] cellular telephone in which a female caller warned of an inappropriate relationship between [REDACTED] and [REDACTED]. [REDACTED] told [REDACTED] it sounded like the same person made all of the calls.
- The first of these calls occurred on October 20, 2009. The caller stated "watch out" and "[REDACTED] having an affair with [REDACTED]."
- The second call occurred the following week near the end of October 2009 when [REDACTED] [REDACTED] and [REDACTED] were [REDACTED]. Again, the female caller warned [REDACTED] to "watch out."
- Between the time of the second call, in late October 2009, and April 2010, [REDACTED] [REDACTED] received to [REDACTED] cellular telephone a number of hang-up calls in which no caller identification information was displayed. [REDACTED] considered these calls to be harassing and contacted a friend with the [REDACTED],

██████████ The ██████████ officer told ██████████ that there was nothing they could do unless ██████████ life was being threatened, and ██████████ did not know if an official report was filed.

- On or about April 10, 2010, and possibly as early as late March 2010, a few days to a week before ██████████ and ██████████ left for another out-of-town conference, ██████████ received another anonymous call from the female. The female stated, “██████████,” and made a reference to ██████████ being in ██████████ office ██████████. ██████████ was very frustrated with the calls at this point, and ██████████ told that it was ██████████.
- During one of the anonymous calls, the female caller told ██████████ “██████████ is in there again.”
- ██████████ does not know who might have made the calls. ██████████ but ██████████ ██████████.
- ██████████ hypothesizes that the caller either obtained ██████████ cellular telephone number from calling ██████████, where the recording mentions the number, or from accessing ██████████, which is available to the public and ██████████. ██████████ thinks ██████████ is telling the truth about the calls.

██████████ immediate supervisor, was interviewed on May 10, 2010, and August 2, 2010. ██████████ knowledge of the anonymous calls is limited to third-hand information ██████████ received from ██████████ and, while not as detailed, generally corresponded with ██████████ statements to the OIG. ██████████ thinks ██████████ might have been “fishing” when ██████████ confronted ██████████ about the telephone calls.

██████████ was asked on May 17, 2010, to attempt to obtain additional information concerning the dates and times of the calls, including reviewing bills and logs from ██████████ cellular telephone provider, but on May 24, 2010, ██████████ responded via email that ██████████ was “not able to pinpoint dates or time further than previously discussed.” (Attachment 2) On or about September 7, 2010, ██████████ left a voicemail in response to an OIG email and telephone message requesting a second interview with ██████████. In the voicemail left by ██████████ with the OIG, ██████████ indicated ██████████ no longer wished to cooperate with this investigation.

FEC telephone records were obtained for analysis to determine if any of the alleged calls originated from FEC telephones. Several calls to ██████████ cellular telephone were found, but the analysis was not helpful in that the records did not identify the extension that dialed the number and, because of the dates and times of the calls, it is likely those found reflect ██████████.

██████████ calling ██████████. It is also possible that the anonymous calls may not have been placed from the FEC telephone system. There is no other currently known evidence to substantiate ██████████ statements concerning the anonymous calls.

B. Computer Breach Involving April Email

██████████ stated in ██████████ initial email of May 5, 2010, "I also believe that someone has accessed ██████████ email and has shared information with me that nobody else could know. [██████████] and I discussed this today and ██████████ is going to speak with your IT department regarding the situation." During ██████████ interview the following day, on May 6, 2010, ██████████ brought up the April email and stated the following:

- ██████████ received a plain envelope with a ██████████ postmark that had been mailed to ██████████ in ██████████. The envelope contained a letter concerning "personal stuff" between ██████████ and ██████████. There was nothing else in the envelope.
- ██████████ was upset about the correspondence. ██████████ ██████████ ██████████ and did not tell ██████████ about the letter or mention its contents.

██████████ provided information about the April email during ██████████ interviews on May 5, May 11, and August 9, 2010. During those interviews, ██████████ stated the following:

- On Wednesday, May 5, 2010, ██████████ approached ██████████ early in the morning as ██████████ was getting ready for work and said, "I need to show you something."³ ██████████ showed ██████████ the April email, dated April 1, 2010, from ██████████ to ██████████. ██████████ knew what it was as soon as ██████████ saw it, and noticed it had what appeared to be a horizontal streak of toner across the top and had been folded into three parts as if it had been in an envelope; ██████████ did not see an envelope. ██████████ told ██████████ it had been sent to ██████████ at ██████████ the previous week. Further, ██████████ stated the following regarding the May 5 events:

██████████ told ██████████ that ██████████ was tired of being harassed and now ██████████, " and then said "I'm done with all this" and "I want it all to stop." ██████████ continued, "It seems like someone's in your email," and ██████████ "

³ In earlier interviews with the OIG soon after the incident, ██████████ confirmed the date it took place. However, during ██████████ August 9, 2010 interview, which was more than three months after the incident, ██████████ thought it had occurred in mid- to late April 2010.

mentioned seeking help from someone at the FEC concerning a possible breach of FEC email account, but did not mention the OIG specifically at this point.

then and went and asked what had done with the April email. replied, " , " to which asked why would do that if wanted someone at the FEC to help. replied, ."

asked about the envelope in which the April email had arrived, and replied that opened it.

- has not given anyone access to FEC email account. It is unlikely that anyone would be able to guess passwords, and has not written them down. Anyone attempting to access FEC email account would need password.
- was issued an FEC PCD in and received no special training or computer security instructions, although the PCD's box contained operating instructions. did not know that it was possible to lock the FEC-issued PCD, as the lockout time was set by the FEC ITD and could not be changed. usually keeps FEC-issued PCD turned off and charging in when at home.
- was issued a .
- In August or September 2009, told that someone put four printed emails between and the FEC official concerning a work-related matter on office chair. While some of the emails had been forwarded to and , the , only and the FEC official had access to all the emails which had been left on the chair. This left to speculate that someone had accessed FEC email account.

During the analysis of ██████████ FEC email account, a copy of the April email was retrieved from the sent folder of ██████████ FEC email account. The computer analyses revealed the following:

- ██████████ and ██████████ were the only ones that have ever had access to the email programs of their respective FEC email accounts.
- The April email was originally sent electronically from ██████████ FEC email account to ██████████ FEC email account on Thursday, April 1, 2010, at 6:31 p.m., and there were no other recipients.
- On Sunday, April 4, 2010, at 1:24 p.m., the April email was forwarded electronically from ██████████ FEC email account sent folder via ██████████ FEC-issued PCD to an email account identified as ██████████. (Attachment 3) This is the same email account used by ██████████ when ██████████ filed the initial complaint.⁴
- There are no indications that ██████████ and ██████████ respective FEC email accounts were broken in to.

██████████ was shown a copy of the April email obtained through the analysis of ██████████ FEC email account during ██████████ August 9, 2010 interview. ██████████ verified it was a copy of the same email ██████████ had shown ██████████ on May 5, 2010, except that the one ██████████ confronted ██████████ with had smaller print and an FEC logo at the top, as well as the aforementioned toner streak and folds. ██████████ initialed and dated the copy that was shown to ██████████ (Attachment 4) When confronted in ██████████ August 9, 2010 interview, with the facts concerning date, time and email address, to which the April email was sent from ██████████ FEC-issued PCD, ██████████ stated the following and provided follow-up information that included:

- *The only people who would have had access to ██████████ FEC-issued PCD on that day and at that time [April 4, 2010, 1:24 p.m.] would have been ██████████ and ██████████.*
- ██████████ *did not forward the April email to ██████████ email, and does not know who would have done it.*

⁴ According to ██████████ ██████████ is the only person who has access to or the password for the ██████████ email account. The account has ██████████ first initial because the ██████████ is in ██████████ name; ██████████ does not know why ██████████ used a ██████████ when setting up the account address.

██████████ was questioned as to ██████████ knowledge of the April email during ██████████ interviews on May 10, 2010, and August 2, 2010. ██████████ knowledge of the April email is limited to third-hand information ██████████ received from ██████████ and, while not as detailed, generally corresponded with ██████████ statements to the OIG. ██████████ stated that it “██████████” that ██████████ would consider making a complaint to the OIG but destroy evidence by burning the email. ██████████ denied printing out or forwarding the April email to anyone else.

C. Previous Attempts to Access ██████████ Electronic Communications

The investigation produced information that ██████████ had a pattern of attempting to access ██████████ personal and business electronic communications, including one known attempt by ██████████ to access ██████████ FEC-issued PCD. In ██████████ interviews on May 11 and August 9, 2010, ██████████ stated the following:

- *In the late summer of 2009, ██████████ found out about ██████████ ██████████ had with ██████████. ██████████ used the history view on the ██████████ shared personal home computer to access ██████████ ██████████ electronic mail account without ██████████ knowledge.⁵*
- *In July 2009, ██████████ personal PCD began unintentionally recording when the record function was accidentally activated. The personal PCD began recording in 10 minute increments throughout the day, including during a conversation ██████████ had with ██████████. ██████████ is not aware the recording was made. A few months later, in October 2009, ██████████ was using ██████████ personal PCD and noticed that there were recordings on it. ██████████ asked ██████████ about them, and ██████████ said ██████████ was unaware of their existence. Later, ██████████ obtained and accessed ██████████ personal PCD without ██████████ knowledge and listened to the recordings.*
- *One night between October 2009 and January 2010, ██████████ woke up ██████████ around ██████████ and said, ██████████ ██████████ said, “██████████ I just tried to get into your [FEC-issued] Blackberry.” ██████████ asked why, and ██████████ stated ██████████ ██████████” and “██████████” ██████████ said the FEC-issued PCD shut itself down after tried too many password attempts. ██████████ told ██████████ “██████████” and asked if ██████████ actions had anything to do with the anonymous calls. ██████████ replied, “██████████.” ██████████ said, “██████████” then said “██████████” and “██████████”*

⁵ ██████████ stated ██████████ did not share ██████████ password for this personal email account with anyone, including ██████████

.” [REDACTED] said, “[REDACTED].” [REDACTED] replied, “[REDACTED].” [REDACTED] asked [REDACTED] what [REDACTED] should do now that [REDACTED] FEC-issued PCD had shut down, and then [REDACTED] took [REDACTED] at [REDACTED] word that [REDACTED] was unable to access the FEC-issued PCD.

- The morning after [REDACTED] told [REDACTED] [REDACTED] had attempted to access [REDACTED] FEC-issued PCD, [REDACTED] told [REDACTED] about the incident, and [REDACTED] told [REDACTED] that if [REDACTED] just hooked it up to the USB port on [REDACTED] computer it would “resynch” itself and restore everything. [REDACTED] tried this, and it worked. [REDACTED] did not notify anyone else, including the ITD Help Desk, about the attempted breach of [REDACTED] FEC-issued PCD. [REDACTED] did not have to change [REDACTED] password at that time, and [REDACTED] did not elect to do it since [REDACTED] did not breach it. [REDACTED] changes [REDACTED] FEC-issued PCD password whenever [REDACTED] is prompted, and has changed it twice since the incident.
- Although [REDACTED] could not remember the approximate date, [REDACTED] once found [REDACTED] FEC-issued PCD [REDACTED] the email screen pulled up instead of the normal “front” screen. This indicated to [REDACTED] that someone may have recently accessed [REDACTED] FEC-issued PCD because the automatic thirty minute timeout and lock had not yet activated. [REDACTED] did not bring this to [REDACTED] attention because [REDACTED] was not sure of what had happened.

[REDACTED] was questioned as to [REDACTED] knowledge of [REDACTED] attempts to access [REDACTED] personal and business electronic communications during [REDACTED] interviews on May 10, 2010, and August 2, 2010. [REDACTED] knowledge of [REDACTED] attempts to access [REDACTED] personal and business electronic communications is limited to third-hand information [REDACTED] received from [REDACTED] and, while not as detailed, corresponded with [REDACTED] statements to the OIG.

D. Relevant Computer Security Training

According to the FEC ITD, [REDACTED] completed computer security awareness training through the FEC’s Skillport training software program in 2007, 2008 and 2009, and had completed Privacy Act training through Skillport in 2010. The 2007, 2009 and 2010 training included the Rules of Behavior. (Attachment 5) Rule of Behavior number 18 requires employees to protect “FEC computing resources from theft or loss,” and to “take particular care to protect any portable devices” such as FEC-issued PCDs. Rule of Behavior number 22 requires employees to “[p]romptly report all security incidents in accordance with FEC policy.”

The 2008 security training included modules on complying with ITD security policies (Attachment 6) and password security (Attachment 7). The ITD security policy module contained a

slide titled “58A FEC Information System Security Program Policy (Responsibility section),” which stated employees must “[t]ake personal responsibility to safeguard and protect information covered in this policy” and “[n]otify the FEC Help Desk and Information Systems Security Manager when a security problem is discovered.” The password security module contained a slide titled “Password DO’S & DON’TS,” which stated under the “DO’S” that employees should “[r]eport security incidents immediately.”

During [REDACTED] interview on August 9, 2010, [REDACTED] was shown, and initialed, copies of Information System Security Program Policy 58A § 4.a.i (Attachment 8), covering personal responsibility for safeguarding and protecting computer information in general, and Personal Communication Devices Security Policy 58-4.4 § 2.k (Attachment 9), which states, “Any FEC-issued PCD must be secured at all times.” [REDACTED] stated [REDACTED] is generally familiar with these concepts, but not the specific policies. [REDACTED] stated [REDACTED] was never directly informed of Policy 58-4.4 when [REDACTED] was issued [REDACTED] FEC PCD or anytime afterward.

V. Findings

The OIG investigation resulted in the following findings:

- The April email had been forwarded from [REDACTED] FEC-issued PCD to [REDACTED] email at [REDACTED] on April 4, 2010, at 1:24 p.m., and only [REDACTED] and the [REDACTED] would have had access to [REDACTED] FEC-issued PCD at that time. However, due to [REDACTED] decision to terminate [REDACTED] cooperation in the investigation and not make himself available for further interviews, the OIG was unable to conclusively establish whether [REDACTED] had accessed [REDACTED] FEC-issued PCD and forwarded the April email to [REDACTED] personal email account. For the same reason, the OIG was unable to conclusively establish whether [REDACTED] knowingly and willfully falsified or concealed a material fact or made any materially false, fictitious, or fraudulent statement or representation concerning the April email in connection with this investigation.
- Due to [REDACTED] decision to terminate [REDACTED] cooperation in the investigation and not provide more detailed cellular telephone records or make himself available for further interviews, the OIG was unable to develop further information concerning the anonymous telephone calls.
- [REDACTED] did not notify the FEC Help Desk as required by FEC Information System Security Program Policy 58A § 4.a.iii and Rule of Behavior number 22 following [REDACTED] admission that [REDACTED] had tried to access [REDACTED] FEC-issued PCD, and that resulted in a lockout of the PCD. However, this finding is

partially mitigated in that FEC Information System Security Program Policy 58A § 4.a.iii and Rule of Behavior number 22 do not explicitly specify that attempted breaches of FEC computer equipment and systems fall under the definition of “security problem” and “security incident,” respectively.

- In light of ██████ attempt to improperly access ██████ FEC-issued PCD, ██████ did not take reasonable steps to keep ██████ FEC-issued PCD secured while at home on April 4, 2010, as required by FEC Personal Communication Devices Security Policy 58-4.4 § 2.k and Rule of Behavior number 18. While leaving an FEC-issued PCD turned off and charging in a common area of an employee’s residence that is only accessible to immediate family members might otherwise be considered reasonable so long as the residence itself is properly secured, once ██████ became aware that ██████ had attempted to breach the FEC email system, ██████ should have taken additional steps to prevent possible future attempted breaches by ██████ including placing ██████ FEC-issued PCD in a more secure location ██████ that was only accessible to ██████ and ensuring the device was locked after each use.⁶ However, this finding is partially mitigated in that ██████ did not receive proper training from ITD in how to lock a PCD.
- ITD should have provided training to ██████ on PCD security when ██████ was issued a FEC PCD, and should have provided ██████ with a copy of Personal Communication Devices Security Policy 58-4.4.
- FEC Information System Security Program Policy 58A § 4.a.iii and Rule of Behavior number 22 do not use consistent terminology and do not explicitly state that an attempt to breach a FEC computer system is to be considered a reportable “security incident” and “security problem.”

VI. Recommendations

Based on these findings and a review of FEC Information System Security Program Policy 58A and FEC Personal Communication Devices Security Policy 58-4.4, the OIG recommends that management consider the following:

- ITD should provide general and PCD security training and copies of ITD security policies each and every time a PCD is issued to a FEC employee or contractor.

⁶ FEC Mobile Computing Security Policy 58-4.3 § 2.d states, “All portable computing devices should be locked in a secured area at the end of the workday.” Absent circumstances such as those present in this matter, one could possibly interpret the term “secured area” to be a secured area in a residence.

- Management should reconcile the terms “security problem” in FEC Information System Security Program Policy 58A § 4.a.iii, and “security incident” in the Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and Systems Resources, to use consistent terminology and be clearer in including *attempts* to access passwords, FEC computing devices or information contained therein.
- Management should consider whether any action is necessary in regards to [REDACTED] [REDACTED] for failing to report a security problem or incident, and for not adequately securing [REDACTED] FEC-issued PCD.
- FEC management should provide a response to the Inspector General within 60 days of this report documenting their action(s) taken or status of the recommendations contained in this report.


VII. Privacy Act and Freedom of Information Act Notice

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENTS

Attachment	Description
1	██████████ original complaint email, dated May 5, 2010
2	██████████ email chain, dated May 24, 2010
3	April email as found during analysis of ██████████ FEC email account, dated April 1, 2010
4	██████████ initialed copy of April email, initialed August 9, 2010
5	Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and Systems Resources
6	FEC Mandatory Security Awareness Training 2008 – Complying with IT Security Policies
7	FEC Mandatory Security Awareness Training 2008 – Password Security
8	██████████ initialed copy of FEC Information System Security Program Policy 58A, initialed August 9, 2010
9	██████████ initialed copy of FEC Personal Communication Devices Security Policy 58-4.4, initialed August 9, 2010

Attachment No. 1

 original complaint email
dated May 5, 2010

Case Number INV-10-02



[REDACTED]
05/05/2010 08:53 AM

To oig@fec.gov

cc

bcc

Subject Good morning

History: This message has been replied to and forwarded.

My name is [REDACTED] and I'm [REDACTED]. I'm not sure where else to turn and hope I've reached the right people to help.

I have been contacted repeatedly (anonymously) regarding the [REDACTED] between [REDACTED] and [REDACTED]. The nature of this contact is to apparently alert me about the nature of [REDACTED] and they expressed that [REDACTED]. I have tried without success to trace the phone calls but have not been able to determine their origin. This contact has happened around the time of [REDACTED] and when they are in private meetings together. I also believe that someone has accessed [REDACTED] email and has shared information with me that nobody else could know. [REDACTED] and I discussed this today and [REDACTED] is going to speak with your IT department regarding the situation.


[REDACTED] also told me there was a complaint about the [REDACTED] recently and this furthers my concern. I hope there is something that can be done about this since it's causing [REDACTED] and could potentially affect an otherwise [REDACTED].

I would appreciate being kept in the loop and know if there is anything I can do to help.

Thank you for your time.

[REDACTED]

Attachment No. 2

 email chain
dated May 24, 2010

Case Number INV-10-02

[Redacted]

05/24/2010 10:36 AM

To jhatfield@fec.gov

cc

bcc

Subject Re: Phone calls

History: This message has been forwarded.

Who	Date	Time	Subject
[Redacted]			

Mr. Hatfield,

Good morning and I'd like to apologize for not getting back to you sooner.

After trying to recall further details regarding date and times of the 2 calls when I was spoken to, I'm sorry to say that I'm not able to pinpoint dates or time further than previously discussed. The 3rd incident I mentioned to you was a series of unknown calls which there was nobody on the other end so therefore I can't really say if they were related. During this period of time I was on guard and assumed the worst every time the phone rang. It's an awful feeling when I start [Redacted] I hope you understand that these incidents created a great deal of [Redacted] and for this reason I decided to not revisit the issue with [Redacted]. As I may have mentioned in our conversation [Redacted] and [Redacted] to the situation.

Thank you again for your attention to this matter.

Best Regards,

[Redacted]

- >
- > Thank you, I look forward to receiving any additional information you can provide on the phone calls you received.
- >
- > Thank you.
- > -Jon
- >
- >
- > _____
- > Jon A. Hatfield
- > Deputy Inspector General
- > Federal Election Commission
- > Office of Inspector General
- > 999 E Street, NW

> Washington, DC 20463
> (202) 694-1015 (office)
> (202) 501-8134 (fax)
> <http://www.fec.gov/fecig/fecig.shtml>

>
>
> [REDACTED]
> 05/17/2010 12:10 PM

> To
> "jhatfield@fec.gov" <jhatfield@fec.gov>
> cc
> Subject
> Re: Phone calls

>
>
>
> I think my last message was sent before complete. I will get any
> information requested and get back to you upon my return. I apologize
> for the confusion, I'm checking and sending email from my mobile
> phone.

> Thank you

> [REDACTED]

> On May 17, 2010, at 9:01 AM, jhatfield@fec.gov wrote:

> [REDACTED]
> Would you have more information on the timing of the harassing
> telephone calls you mentioned? It is my understanding you received
> at least three such calls, in which you stated a woman made
> harassing comments to you. You stated these calls were placed in
> (1) October 2009; (2) [REDACTED] (3) and
> sometime in 2010. If you could search your cell phone call logs and/
> or bill and provide a more precise day/time of the calls, this would
> be helpful. Absent any such records, if you can remember the day/
> month, this would be helpful. Also, time of day.

> Thank you.
> -Jon

>
> _____
> Jon A. Hatfield
> Deputy Inspector General
> Federal Election Commission
> Office of Inspector General
> 999 E Street, NW
> Washington, DC 20463
> (202) 694-1015 (office)
> (202) 501-8134 (fax)
> <http://www.fec.gov/fecig/fecig.shtml>

> [REDACTED]
> 05/05/2010 06:18 PM
>
>
> To
> jhatfield@fec.gov
> cc
> Subject
> Re: Good morning
>
>
>
>
>
> I understand that [REDACTED] has been dealing with this all day.
> Tomorrow I have meetings from 9:30 until 1pm or so. Anytime after
> that should be fine, thank you.
>
> On May 5, 2010, at 5:52 PM, jhatfield@fec.gov wrote:
>
> [REDACTED]
> I am in receipt of your email. I will contact you tomorrow on the
> number you have listed below.
>
> Thank you.
> -Jon
>
>
> _____
> Jon A. Hatfield
> Deputy Inspector General
> Federal Election Commission
> Office of Inspector General
> 999 E Street, NW
> Washington, DC 20463
> (202) 694-1015 (office)
> (202) 501-8134 (fax)
> <http://www.fec.gov/fecig/fecig.shtml>
>
> [REDACTED]
> 05/05/2010 08:53 AM
>
>
>
> To
> oig@fec.gov
> cc
> Subject
> Good morning
>
>
>
>
>
>
>
> My name is [REDACTED] and I'm [REDACTED]. I'm not

> sure where else to turn and hope I've reached the right people to
> help.
>
> I have been contacted repeatedly (anonymously) regarding the
> [REDACTED] between [REDACTED] and [REDACTED]. The nature of
> this contact is to apparently alert me about the nature of their
> [REDACTED] and they expressed that it is [REDACTED]. I
> have tried without success to trace the phone calls but have not been
> able to determine their origin. This contact has happened around the
> time of [REDACTED] and when they are in private meetings
> together. I also believe that someone has accessed [REDACTED] email and has
> shared information with me that nobody else could know. [REDACTED] and I
> discussed this today and [REDACTED] is going to speak with your IT
> department regarding the situation.
>
> [REDACTED] also told me there was a complaint about [REDACTED]
> recently and this furthers my concern. I hope there is something that
> can be done about this since it's causing [REDACTED] and
> could potentially affect an otherwise [REDACTED]
> career.
>
> I would appreciate being kept in the loop and know if there is
> anything I can do to help.
>
> Thank you for your time.
>
> [REDACTED]
>
>
>
>
>
>
>

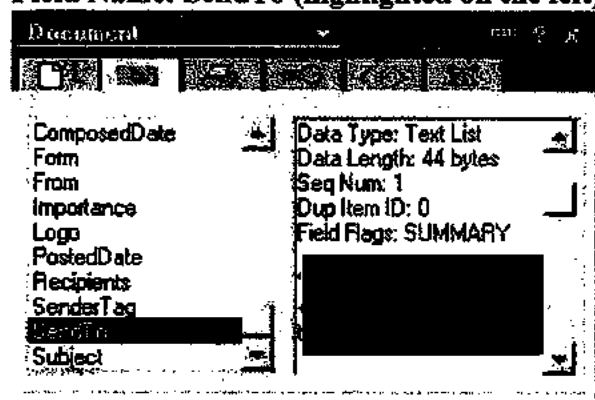
Attachment No. 3

Questioned Email as found during analysis of [REDACTED] FEC email account
dated April 1, 2010

Case Number INV-10-02

The next TAB is the **Fields Tab**, which reveals the message headers.

Field Name: SendTo (highlighted on the left)

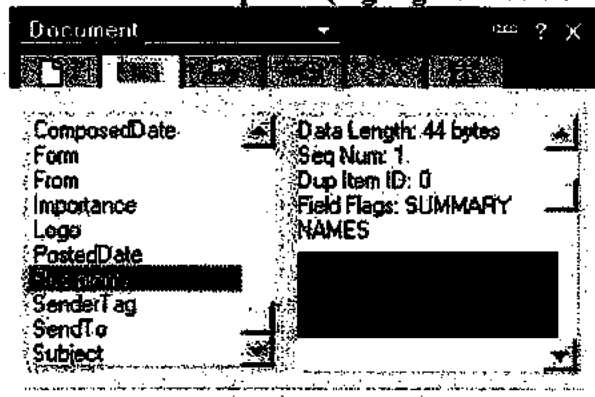


Results (listed below from the right)

Field Name: SendTo
Data Type: Text List
Data Length: 44 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY



Field Name: Recipients (highlighted on the left)

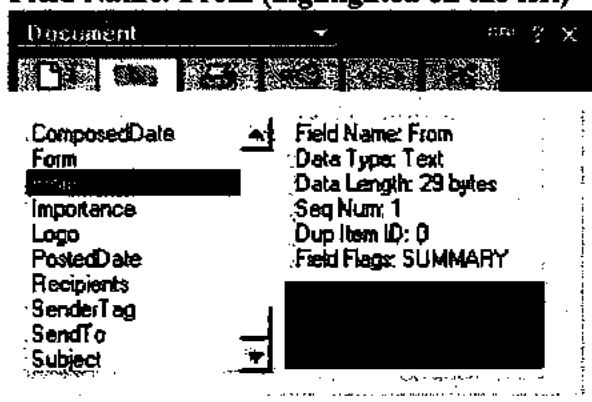


Results (listed below from the right)

Field Name: Recipients
Data Type: Text List
Data Length: 44 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY NAMES



Field Name: From (highlighted on the left)

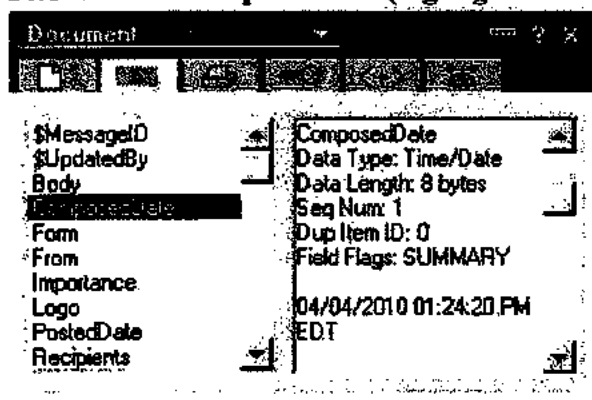


Results (listed below from the right)

Field Name: From
 Data Type: Text
 Data Length: 29 bytes
 Seq Num: 1
 Dup Item ID: 0
 Field Flags: SUMMARY



Field Name: ComposedDate (highlighted on the left)




Results (listed below from the right)

Field Name: ComposedDate
 Data Type: Time/Date
 Data Length: 8 bytes
 Seq Num: 1
 Dup Item ID: 0
 Field Flags: SUMMARY

04/04/2010 01:24:20 PM EDT

Attachment No. 4

 initialed copy of Questioned Email
initialed August 9, 2010

Case Number INV-10-02

Attachment No. 5

**Rules of Behavior and Acceptable Use Standards for Federal Election Commission
Information and Systems Resources**

Case Number INV-10-02

Rules Of Behavior and Acceptable Use Standards For Federal Election Commission Information and Systems Resources

The following statements reflect generally accepted best practice within the Federal government, and are provided to serve as a ready reference that will help FEC employees remain in compliance with FEC Information System Security Program policies.

1. FEC systems are to be used primarily for official business.
2. FEC information must not be disclosed to unauthorized individuals.
3. FEC employees must not research, or change any account, file, record, or application not required to perform their job.
4. No one can be allowed to enter FEC facilities without proper authorization.
5. Do not disclose the telephone number(s) or procedure(s) that permit system access from a remote location.
6. Do not dual-home your computer when accessing FEC networks. Connection to a FEC network *and* simultaneous connection to the Internet through a second, separate communications channel exposes the FEC network to unacceptable risks.
7. Do not use an FEC computer or terminal on behalf of another person. If asked by another person to access sensitive information, verify with the person's immediate supervisor that the request is valid.
8. Protect your password from disclosure. Specifically:
 - a. Password length must be at least eight characters, must consist of a mix of upper- and lower-case letters, and must include at least one number and one special character.
 - b. Passwords must be changed at least once every 180 days, OR SOONER if someone else knows the password.
 - c. Do not share your password with others or reveal it to anyone, regardless of his/her position in or outside the FEC. Everything done under your password will be regarded as having been done by you.
 - d. Do not post your password in your area.
 - e. Do not program your login or password into automatic script routines or programs, unless allowed by FEC policies and standards.
 - f. Do not use another person's password.
 - g. Do not accept a password that is not delivered via secure means.
 - h. Notify your immediate supervisor and the FEC ISSM of any violation of this rule.
9. Log off or lock the computer anytime you leave your computer or terminal.
10. Retrieve hard copy printouts and faxes sent to you in a timely manner, and ensure that they are stored in manner commensurate with their sensitivity.
11. Do not use personal equipment or software for FEC business without proper approval.
12. Update the anti-virus software on any FEC-owned or personal computing devices that you use for FEC business. This software must not be disabled for any reason.
13. Do not modify the operating system configuration on FEC computing resources without proper approval.

14. Do not install or use unauthorized software on FEC computing resources. Do not use gameware, freeware, shareware or public domain software on FEC computers without authorization and without scanning it for viruses.
15. Observe all software license agreements and copyright laws.
16. Do not move equipment, add or exchange system components without authorization by the appropriate approval of ITD.
17. Protect FEC computing resources from hazards such as liquids, food, smoke, staples, paper clips, etc.
18. Protect FEC computing resources from theft or loss; take particular care to protect any portable devices and media entrusted to you, such as laptops, cell phones, palm-top computers, disks, CDs, and other portable electronic storage media.
19. Protect information storage media from exposure to electrical currents, extreme temperatures, bending, scratches, fingerprints, fluids, smoke, etc. Ensure that media is secured when not in use based on the sensitivity of the information contained, and practice proper labeling procedures.
20. Use of government e-mail and Internet accounts is a privilege, not a right. Specifically:
 - a. There is no expectation of privacy in FEC electronic mail communications.
 - b. Do not send or store inappropriate material using your FEC e-mail or Internet accounts. Do not originate or forward chain letters or hoaxes. Pornography, inappropriate language, gender, racial and religious bias, and anything that may be viewed as sexual harassment will not be tolerated.
 - c. Do not auto-forward e-mail from your FEC account to a personal e-mail account.
21. Back up data and store it in accordance with FEC business continuity plans and policies.
22. Promptly report all security incidents in accordance with FEC policy.

Attachment No. 6

FEC Mandatory Security Awareness Training 2008
Complying with IT Security Policies

Case Number INV-10-02

THE FEDERAL ELECTION COMMISSION
Mandatory Security Awareness Training
2008



**Complying with IT Security
Policies**

2007 Privacy Audit

- One 2007 Privacy Audit finding was that there were numerous instances where FEC employees failed to comply with IT Security policies. Specifically:
 - Employees left usernames & Passwords written on notes within proximity to their computers.
 - Employees left USB 2-factor encryption authentication tokens unsecured in their laptops.

FEC Rules of Behavior and Acceptable Use Standards

- **Section 8.d**

Protect your password from disclosure. Specifically, do not post your password in your area.

- **Section 18**

Protect FEC computing resources from theft or loss; take particular care to protect any portable devices and media entrusted to you, such as laptops, cell phones, palm-top computers, disks, CDs, and other portable electronic storage media.

Mobile Computing Security Policy

- Section 2.a

Portable computing devices and associated peripherals issued by the FEC should be viewed as government property that must be adequately protected from theft;

Commission Directive 58 (General Policy section)

The Commission's large scale investment in computer technology has greatly enhanced our capabilities in the agency's disclosure program, our audit and enforcement programs, and our day-to-day administrative activities. Our Information Technology Architecture (ITA) is largely decentralized and considerable autonomy is therefore afforded individual staff members (hereafter, "end users"). This in turn, confers considerable responsibility on end users to ensure that information systems are used appropriately and protected from loss, misuse, or unauthorized access. This includes a responsibility to minimize the FEC vulnerability to inadvertent or malicious systems failures, to respect software licensing and copyright laws, and to protect information stored on agency computers.

58A FEC Information System Security Program Policy (Responsibility section)

All FEC employees, consultants, subcontractors, and other authorized users of company or client information:

1. Take personal responsibility to safeguard and protect information covered in this policy;
2. Read the FEC Rule of Behavior and Acceptable Use standard so as to understand how to properly handle and protect FEC information and systems in a manner consistent with established FEC policies, standards, and procedures; and
3. Notify the FEC Help Desk and Information Systems Security Manager when a security problem is discovered.

The FEC Warning Banner

This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Federal Election Commission (FEC) only for authorized use in accordance with FEC Directive 58, Electronic Records, Software and Computer Usage, and FEC Policy No. 58A, Information System Security Program Policy. All FEC computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored. Therefore, there should be no expectation of privacy with respect to your use of this system. By logging into this FEC computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized, unauthorized or illegal, collected during monitoring may be used and subject you to civil, administrative or other adverse action, and/or criminal prosecution.

The Bottom Line!

FEC IT security policies and Privacy Protection Policies, apply to anyone who accesses a Commission computer system, this includes all employees and vendors/contractors and related personnel.

These policies are designed to not only protect government information but also your private personal information. Failure to adhere to FEC IT security policies and Privacy Protection policies may lead to civil, administrative or other adverse action, and/or criminal prosecution.

Attachment No. 7

**FEC Mandatory Security Awareness Training 2008
Password Security**

Case Number INV-10-02

The Federal Election Commission Mandatory 2008 Security Awareness Training

Password Security

We need your help

The IT department uses the latest technology and techniques to maintain the highest level of security possible, but we can't do the job without your help. Every employee plays a critical role in keeping our computer network secure.

One of the greatest security vulnerabilities lies in the improper or ineffective use of passwords. Here are some important guidelines to keep in mind.



What is a weak password?

A weak password:

- ▶ Contains fewer than six characters
- ▶ Is a word found in a dictionary (English or foreign)
- ▶ Is a common usage word such as:
 - Passwords containing the user ID in any form
 - Names of family, pets, friends, or co-workers
 - Birthdays and personal information, such as addresses and phone numbers
 - Any of the above spelled backward
 - Any of the above preceded or followed by a digit (secret1, 1secret) or the same letter (ssecret, secrett)

What is a strong password?

A strong password:

- ▶ Contains digits, symbols, and uppercase and lowercase characters. For example:

a-z, A-Z, 0-9, !@#\$%^&*()_+|~-=\`{}[]:"';<>?,./

- ▶ Is at least eight characters long
- ▶ Isn't a word in any language, slang, or dialect
- ▶ Isn't based on personal information, names of family, etc.

Password Examples

Do not use these as your password; they're just examples!

Good one-time use password (> 16 char)

- Example: e-mail a file-level protected Excel 2003 workbook

1. "ThisIsMy1timePasswordx2791"

A concatenated sentence plus extension

2. "CNET!2005Jun@hipaa#2791"

<company> [Shift]1 <date> [Shift]2 <type> [Shift]3 <extension>

Good normal use password (> 8 char)

- Example: application login password

#win8hir05

[Shift]3 <first 3 letters of your firstname> <random number>

<last 3 letters of your lastname> <year>

Use a pattern that you !can remember without writing it down!

Loss of Information

The time to crack/hack passwords with respect to the password length and its complexity. The search speed supposedly equals 100,000 passwords per second (a very decent speed).

Password length /charset	26 (no case, letters only)	36 (no case, letters & digits)	52 (case sensitive)	96 (all printable)
4	0	0	1 min	13 min
5	0	10 min	1 hr	22 hr
6	50 minutes	6 hrs	2.2 days	3 months
7	22 hrs	9 days	4 months	23 yrs
8	24 days	10.5 months	17 yrs	2,287 yrs
9	21 months	32.6 yrs	881 yrs	219,000 yrs
10	45 yrs	1,159 yrs	45,838 yrs	21 million yrs

Password DO'S & DON'TS

DO'S:

- Keep your user ID and password to yourself
- Use antivirus software (both at home and at work)
- Screen-lock or log off your computer desktop when you are away from the computer
- Report security incidents immediately

DON'TS:

- Reveal your password to anyone over the phone, e-mail, or IM
- Share your password with your boss, family members, or a co-worker while you're on vacation
- Reveal a password on questionnaires or security forms
- Use the "Remember Password" feature of applications in any public computer (conference room, airport, Internet café, etc).

The FEC Password Standard

- ▶ Standard location: [[FEC Password Standard](#)]
- ▶ Highlights
 - Minimum password length is 8 characters
 - Complexity is required, must consist of 1 upper & lower case character, at least 1 number, and 1 special character.
 - All user passwords (e-mail, login, etc.) must be changed at least every 180 days– no exceptions!
 - A password can't be reused for at least two ½ years
 - After 5 consecutive login failures, the account will be locked and the IT Help Desk must be notified to re-enable
 - IT Support staff must be able to verify the identity of the requestor before resetting the password
 - Temporary passwords must be changed at the next login
 - Sharing passwords is not allowed

Keep your password secret!

- ▶ Treat your passwords and pass phrases with as much care as the information that they protect.
- ▶ Protect any recorded passwords. Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.
- ▶ Never provide your password over e-mail or based on an e-mail request. Any e-mail that requests your password or requests that you to go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted company or individual.
- ▶ Do not type passwords on computers that you do not control. Computers such as those in Internet cafés, computer labs, shared systems, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, bank balances, business mail, or any other account that requires a user name and password. Criminals can purchase keystroke logging devices for very little money and they take only a few moments to install. These devices let malicious users harvest all the information typed on a computer from across the Internet—your passwords and pass phrases are worth as much as the information that they protect.

What to do if your password is stolen.

- ▶ **If it's a work related account,**

Change the password immediately and contact the IT Help Desk at 1255.

- ▶ **If it's a personal account,**


Be sure to monitor all the information you protect with your passwords, such as your monthly financial statements, credit reports, online shopping accounts, and so on. If you notice any suspicious activity that could indicate that someone has accessed your information, change your password and notify authorities immediately.



For more information

Contact the FEC IT Security Officer
at X1266

Attachment No. 8

 initialed copy of FEC Information System Security Program Policy 58A
initialed August 9, 2010

Case Number INV-10-02

Federal Election Commission (FEC)
Information System Security Program Policy

Policy Number: 58A

May, 2004

References

- a. Federal Election Commission Information Technology Security Program Plan, October 1999 (hereby canceled)
- b. Federal Election Commission Directive #58, Electronic Records Software and Computer Usage, January 25, 2007
- c. FEC Personnel Security Policy 58-1.1
- d. FEC Security Training Policy 58-1.2
- e. FEC Information Classification Policy 58-1.3
- f. FEC Hardware and Software Acquisition Policy 58-1.4
- g. FEC Third Party Services Policy 58-1.5
- h. FEC Risk Management Policy 58-2.1
- i. FEC Account Management Policy 58-2.2
- j. FEC Change Management Policy 58-2.3
- k. FEC Certification and Accreditation Policy 58-2.4
- l. FEC User Support Policy 58-2.6
- m. FEC Segregation of Duties Policy 58-2.7
- n. FEC Backup and Recovery Policy 58-2.8
- o. FEC Continuity of Operations/Disaster Recovery Policy 58-2.9
- p. FEC Security Incident Response Policy 58-2.10
- q. FEC Security Review Policy 58-2.11
- r. FEC Logical Access Policy 58-3.1
- s. FEC Applications and Operating System Security Policy 58-3.2
- t. FEC Auditing and Monitoring Policy 58-3.3
- u. FEC Electronic Mail and Internet Security Policy 58-3.5
- v. FEC Malicious Code Policy 58-3.6
- w. FEC Wireless Security 58-3.7
- x. FEC Personally Owned Wireless Connectivity Security Policy 58-37A
- y. FEC Physical Access Control Policy 58-4.1
- z. FEC Media Management Policy 58-4.2
- aa. FEC Mobile Computing/Hardware Security 58-4.3
- bb. FEC Personal Communications Device Security Policy 58-4.4
- cc. FEC Virtual Private Network VPN Policy 58-4.5
- dd.

1. PURPOSE

- a. This policy reissues and revises the existing security policy for the safeguarding of electronic information within Federal Election Commission (FEC) systems. The purpose of this policy is to establish an agency-wide program for protecting FEC information. The goal is to manage the risk to information rather than just "systems", because our information is far more valuable to the FEC than the machines used to process, store or transmit it. This is not to say that computers and other automated assets are not valuable and deserving of protection – they are. However, protecting computer equipment is not an end unto itself, but a part of protecting FEC information. This policy covers all FEC information in electronic or digital format. It also covers any automated system that is used to create, process, store, or transmit electronic information.
- b. This policy assigns responsibility for protecting information and information systems to all those authorized to use FEC information. While certain people have specific duties, be aware that everyone who is granted access to FEC information has a personal responsibility to help protect it.
- c. The agency's goal is to manage risk rather than ignore or avoid risk. Our information security efforts should aim at keeping risks to information confidentiality, integrity, and availability at levels that make sense for FEC, as opposed to either avoiding all risk, or ignoring risk entirely.
- d. What this means is that information risk management must be balanced against business needs; security practices, procedures, and technologies must be cost-effective for FEC. They also need to be balanced in the sense that there is not a single solution for information security; risk management requires a mix of administrative, operational, physical, or technical measures and controls.
- e. It also means that an information life-cycle management approach is important to implementing information security requirements. Information must be protected throughout its life cycle, from creation or collection through processing, analysis, application, storage, transmission, and disposal.

2. APPLICABILITY AND SCOPE

This policy applies:

- a. Enterprise-wide across the FEC.
- b. To anyone granted access to FEC information; this includes employees, subcontractors, consultants, and other service personnel.
- c. To all FEC electronic information regardless of form or format, and includes the following classes of information:
 - i. Sensitive information: Defined in the Computer Security Act of 1987, Title 15 United States Code, and commonly referred to as Controlled Unclassified Information or as Sensitive But Unclassified (SBU);
 - ii. Privacy Data: Any record that is contained in a system of records, as defined in the Privacy Act of 1974, Title 5, United States Code, and information the disclosure of which would constitute an unwarranted invasion of personal privacy;
 - iii. For Official Use Only (FOUO): Information which may be withheld from the public because it falls under exemptions 2-9 in the Freedom of Information Act (FOIA);
 - iv. Public information: Information that has been reviewed and approved for public release.
- d. To all systems that are used to create, process, store, or transmit FEC's electronic information. This includes Agency desktop and mainframe computers, servers, networks and network devices, personal computers; personal digital assistants (PDAs), and any other computing technology that may emerge in the future.
- e. All information systems that handle FEC information must comply with the pertinent requirements of this policy.

3. POLICY

It is FEC policy that:

- a. Information in the possession of FEC is held on behalf of the United States Government and the American public. Only people who have been formally granted access are allowed to use FEC information, and then only in accordance with the terms of this and other FEC information security policies and guidance, or in accordance with public law.
- b. Information is a strategic asset vital to the FEC's ability to carry out its legal mandates and core business processes. As a strategic asset, information has to be protected at a level appropriate to its value, for as long as may be required to protect Agency interests.
- c. Three attributes of FEC information must be protected:
 - i. *Confidentiality*: The confidentiality of FEC and official information, or other information protected by law or regulatory requirements, must be maintained.
 - ii. *Integrity*: Information must be protected from illicit or unintentional destruction or modification so that the integrity of FEC information is assured. Users must have assurance that information has not been improperly modified during processing, storage, or transmission.
 - iii. *Availability*: Information must be available where and when needed to support FEC business operations and missions.
- d. A balanced, cost-effective application of security policies, standards, procedures and technologies is required to protect FEC information and systems, including technical systems security, operational and administrative security, personnel security, and physical security.
- e. Information assurance is an integral part of FEC business processes; as such, it must be addressed at all management levels. FEC information's security must be addressed throughout its life cycle, from creation or collection through processing, analysis, application, storage, transmission, and disposal.

4. RESPONSIBILITIES

- a. All FEC employees, consultants, subcontractors, and other authorized users of company or client information:
- i. Take personal responsibility to safeguard and protect information covered in this policy;
 - ii. Read the FEC Rule of Behavior and Acceptable Use standard so as to understand how to properly handle and protect FEC information and systems in a manner consistent with established FEC policies, standards, and procedures; and
 - iii. Notify the FEC Help Desk when a security problem is discovered.
- b. The FEC Chief Information Officer (CIO):
- i. Sign, issue, and oversee implementation and enforcement of this policy.
 - ii. Review and approve FEC information and AIS security policies. Direct FEC information and AIS standards, manuals, operating procedures, guidelines, and instructions to be developed in conformance with federal guidance and generally accepted good practice;
 - iii. Develop and provide visible support for an Information and AIS security program for all information under FEC jurisdiction;
 - iv. Direct data ownership/custodianship be established for each category of agency information, to include accountability, access rights, and special handling requirements;
 - v. Direct appointment of an FEC Information System Security Officer (ISSO), and direct that he or she receive appropriate training to carry out the duties of this function;
 - vi. Direct funding and resources be programmed for staffing, training, and supporting the FEC security program and for implementing information and information system safeguards;
 - vii. Track identified security deficiencies and incidents to their final resolution; apply resources to help manage risk to an acceptable, cost effective level.
- c. All FEC Managers, Branch Chiefs and Supervisors:
- i. Implement, maintain and provide visible support for an overall information and AIS security program designed to ensure compliance with this policy;
 - ii. Make security policies, standards and procedures available to users so that that they can familiarize themselves with FEC security practices before access they are granted access to FEC information systems;

- iii. Review contracts and, as needed, insert language that requires contractors and consultants to be familiar with and follow FEC security policies, standards and procedures;
 - iv. Ensure that all required safeguards are implemented and maintained; and
 - v. Identify security deficiencies and, where they are serious, take action (e.g., allocate additional resources) to help manage risk to an acceptable, cost effective level.
- d. The FEC Information System Security Manager (ISSO):
- i. Review and approve standards, techniques, systems, and equipment for telecommunications and automated information systems security;
 - ii. Review, approve, and assist with developing all FEC information system security policies, standards, manuals, operating procedures, guidelines, instructions and other programs.
 - iii. Evaluate computer products intended for use by FEC components;
 - iv. Serve as the focal point for technical matters on using computer products and systems and, with FEC computer security testing and evaluation activities, provide technical advice to the FEC components on using products and systems;
 - v. Establish and maintain a computer and information security incident response capability; and
 - vi. Coordinate and manage independent assessments of FEC's information risk management posture with the FEC Chief Information Officer.
 - vii. Provide oversight of third party security contract provisions and compliance; and
 - viii. Establish data ownership/custodianship for each category of agency information.
 - ix. Assist the FEC Chief Information Officer with enforcement of this policy; provide FEC Security Program execution and policy enforcement oversight;
 - x. Coordinate data collection for internal and external security program status reports, audits and reviews;
 - xi. Identify, report and track the status of security deficiencies; track problems to their resolution;
 - xii. Assist the FEC Office of Technology Deputy Chief Information officer with evaluating computer products intended for use by FEC;
 - xiii. Assist the FEC Chief Information officer with developing a formal security model; in coordination with FEC Business Owners, define minimum security standards, procedures and guidelines (to include accountability, access rights, and special handling requirements) for safeguarding FEC information based on classification;

- xiv. Assist the FEC Chief Information officer with reviewing the standards, techniques, systems, and equipment that are relevant to FEC information systems security;
 - xv. Serve as the focal point for all FEC electronic information assurance and related technology security activities; provide information assurance and information systems security advice and support, and disseminate information on threats to FEC information and systems, such as viruses and systems flaws that should be patched;
 - xvi. Keep a list of FEC personnel and their contact information (e-mail, phone numbers) who may need to be notified in case of a computer security incident;
 - xvii. Develop all FEC security policies and standards for review, approval and promulgation;
 - xviii. Manage changes to this policy;
 - xix. Support systems personnel with properly implementing required information system security measures;
 - xx. Serve as the FEC representative for information system security and electronic information assurance to all organizations outside FEC;
 - xxi. Provide oversight of the FEC security training program; help System Owners with obtaining the specialized training they need to perform their security-related functions;
 - xxii. Distribute the FEC Rules of Behavior and Acceptable Use statement to everyone who is authorized to access and use FEC information so that they can read and be familiar with the standard; and
 - xxiii. Perform other duties as assigned in subordinate FEC information system security policies.
- e. The FEC Assistant ISSM (AISSO):
- i. Assist the ISSO with implementing and enforcing the FEC IT Security Program;
 - ii. Carry out the FEC Security Training and Awareness program implementation; develop and provide initial and periodic refresher training for FEC employees on FEC security practices and standards of behavior; and
 - iii. Perform other duties as assigned in FEC information system security policies.
- f. Systems Owners for FEC General Support Systems and Major Applications:
- i. Operate, use, maintain, and dispose of FEC information systems in accordance with internal security policies and practices;
 - ii. Enforce security policies and safeguards for everyone with access to the information system(s) they are responsible for;
 - iii. Periodically review their systems' audit trails;

- iv. Identify security deficiencies and, where the deficiencies are serious begin protective or corrective measures.
- v. Report security incidents in accordance with FEC incident reporting procedures.
- vi. Report the security status of their system to the FEC ISSM as needed;
- vii. Evaluate known vulnerabilities to see if additional safeguards are needed; and
- viii. Maintain a plan for system security improvements and progress towards meeting the goals of this policy.

5. EFFECTIVE DATE AND ISSUANCE

- a. This policy is effective immediately.

6. POLICY CHANGE PROCEDURE

- a. Only the FEC Chief Information officer can authorize changes to this policy. Even if no changes are proposed, this policy will be reviewed at least once every year.
- b. To change this policy:
 - i. Forward a change request to the FEC ISSO for evaluation;
 - ii. The FEC ISSO will recommend approval or disapproval to the FEC Chief Information officer.
- c. The FEC Chief Information officer will make a final determination for the FEC as to which changes to approve.

7. POLICY CRITERIA

- a. All OIT security policies will be signed and dated by the FEC Chief Information officer.
- b. All OIT security policies will be reviewed and updated (if necessary) annually.

8. STANDARDS & GUIDELINE CRITERIA

- a. All OIT security standards and guidelines will be signed and dated by the FEC ISSO.
- b. All OIT security standards and guidelines will be reviewed and updated (if necessary) annually.

Revision Number	Revision Date	Revision Synopsis
1	04/08/10	Updated to include policy, standard, & guideline review process
2	04/08/10	Updated to reflect new policies
3		
4		
5		
6		
7		
8		

Review History


Reviewer	Review Date	Review Synopsis

This procedures were adopted on Month, Day Year



Alec Palmer
Chief Information Officer

Attachment No. 9

 initialed copy of FEC Personal Communication Devices Security Policy 58-4.4
initialed August 9, 2010

Case Number INV-10-02

Federal Election Commission
Personal Communication Devices Security Policy
Policy Number 58-4.4

1. PURPOSE


This policy is designed to:

- a. Satisfy the purposes and policy goals of the Federal Election Commission (FEC) Information System Security Program Policy, Policy Number 58A.
- b. Establish control over the processes to secure Personal Communication Devices (PCD) devices and the FEC information they process, store or transmit. For the purpose of this policy, PCDs are defined to include personal digital assistants (PDA), cellular telephones, laptop wireless cards and pagers.
- c. Establish a base group of PCD users and formalize the approval process for adding additional users.
- d. Maintain control over high-value FEC assets, and safeguard FEC information.

2. POLICY

It is FEC policy that:

- a. PCDs are issued, for operational efficiency, to personnel who need to conduct immediate, critical FEC business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.
- b. The following staff establishes the core group of FEC PCD users:
 - i. Commissioners,
 - ii. Commission Office staff.
 - iii. Staff Director,
 - iv. Deputy Staff Directors
 - v. Office of Inspector General
 - vi. Office of the Chief Finance Officer
 - vii. General Counsel
 - viii. Associate General Counsel

- c. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred. All requests to obtain a FEC PCD from staff other than those specified in section 2(a) must be submitted in writing to the appropriate Deputy Staff Director, or Associate General Counsel for approval. Employees of the Offices of Inspector General and Chief Financial Officer should submit their request to their appropriate manager. Any request must contain justification demonstrating how a FEC PCD is essential to performance of the requestor's duties. Approved requests are to be submitted to the Chief Information Officer (CIO) for processing.
- d. All new hardware, software, and/or related components that provide FEC PCD related connectivity and services for the FEC will be managed by the Information Technology Division (ITD).
- e. The installation of a non-FEC FEC PCD and related hardware, software, and related components not approved by ITD is prohibited.
- f. Prior to initial use or connecting to the FEC's network, all PCD devices and licensed hardware, software and related services must be registered with ITD. No employees or contractors will make modifications of any kind to FEC owned and installed PCD devices without the express approval of ITD.
- g. Non-FEC FEC PCD cannot be connected to an FEC information resource without the written approval of ITD. If approved:
 - i. The FEC will in no way support your non-FEC FEC PCD device. This includes installation, configuration, maintenance and troubleshooting.
 - ii. If it is determined that your non-FEC FEC PCD device is interfering with the configuration and/or security of an FEC information resource the device must be disconnected immediately.
- h. It is the responsibility of any FEC employee and/or contractor who is connecting to the FEC network via a FEC or non-FEC FEC PCD device or similar service to ensure that all components of his/her wireless connection remain secure.
- i. Employees and/or contractors using a PCD device and services for remote wireless access will, adhere to FEC Information Technology Security policies and procedures.
- j. ITD reserves the right to turn off, without notice any access to the network that puts the FEC's systems or data at risk.
- k. Any FEC-issued PCD must be secured at all times. 
- l. FEC-issued PCD devices should not be left unattended while being transported, unless locked in a secure location where not visible (e.g. airport terminal locker, the trunk of a locked car);
- m. If a FEC PCD device is stolen (regardless of where the theft occurs), the device's owner/user (i.e., the person responsible), will:

- i. Notify the Information System Security Officer (ISSO) as soon as possible; and
 - ii. File a police report as soon as possible.
- n. If a FEC PCD device is lost (regardless of where the loss occurs), the device's owner/user (i.e., the person responsible), will notify the Information System Security Officer (ISSO) as soon as possible.
 - o. All assigned portable computing devices, peripherals, related equipment and media are FEC property and are to be returned to the IT Division upon request, or when an employee leaves FEC's employment.
 - p. All FEC PCD devices must be encrypted and/or password protected. FEC's *Password Policy* is relevant here.
 - q. All FEC PCD devices must use a "time-out" function for remote access and mobile devices requiring user reauthentication after a minimum of 30 minutes inactivity.
 - r. Transfer of FEC email to a non-FEC-FEC PCD is prohibited.
 - s. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee.
 - t. PCDs are issued for FEC business. Personal use should be limited to minimal and incidental use. The cost of any personal use is the responsibility of the employee. Appropriate discipline may be taken if it is determined that the rule of minimal personal use has been abused.
 - u. Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle.
 - v. Any employee found to have violated this policy may be subject to disciplinary action that leads to being ineligible for continued use of PCDs. Extreme cases could lead to additional discipline, up to and including termination of employment.

3. RESPONSIBILITIES

- a. All FEC authorized users of FEC information:
 - i. Comply with the terms of this policy; and
 - ii. Report violations of this policy expeditiously to cognizant authority.
- b. The FEC Chief Information Officer:
 - i. Sign, issue, and oversee the implementation and enforcement of this policy;
- c. The FEC Information Systems Security Officer (ISSO):
 - i. Develop and issue technical standards regarding acceptable anti-theft devices; and

- ii. Implement and manage changes to this policy.
 - iii. In coordination with Business Owners and the ISSO, help assess the actual or possible operational impact resulting from PCD device loss, theft or damage;
 - iv. Maintain records by nomenclature and serial number of mobile computing devices that are reported as lost or stolen; and
 - v. In coordination with the ISSO, investigate cost-effective ways to reduce theft threats.
- d. The FEC Assistant ISSO:
- i. Assist the ISSO with implementing this policy as required.
- e. Systems Owners for FEC General Support Systems and Major Applications:
- i. Report lost, stolen, or missing PCD devices immediately in accordance with FEC *Incident Response Policy and Impact Assessment Standards*; and
 - ii. In cases where sensitive information may have been compromised, inform the ISSO.
- f. Deputy Staff Director for Management and Administration
- i. Monitor all program costs for appropriate usage.

This policy was adopted on July 09, 2008



Alec Palmer
Chief Information Officer

Revision History

Revision Number	Revision Date	Revision Synopsis
1	07/11/08	Modified to accurately include the OIG & CFOO
2	2/10	Modifications to reflect OIT reorganization
3		
4		
5		
6		
7		
8		

Review History

Reviewer	Review Date	Review Synopsis
Edward F. Bouling CISO	12/16/09	No update



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CASE CLOSING MEMORANDUM

Case #: INV-11-01	Prepared By: J. Cameron THURBER
Case Title: Alleged Ethics Violation	
Date of Report: January 9, 2012	
Subject: Case Closing	

Hotline Complaint HL-11-02 was opened on September 7, 2011, following the Office of Inspector General's (OIG) receipt on September 1, 2011, of a Hotline complaint referral from the [REDACTED]. The referral alleged that [REDACTED], an [REDACTED] in the [REDACTED], had represented private clients in Internal Revenue Service (IRS) audits, in violation of 18 U.S.C. §§ 203 and 205, and served as an expert witness, in violation of 5 C.F.R. § 2635.805. [REDACTED] had allegedly met with [REDACTED], former [REDACTED], and provided the information leading to the referral. Investigation INV-11-01 was opened on September 7, 2011, in accordance with OIG Hotline Complaint evaluation guidelines.

Interviews were conducted of [REDACTED] and [REDACTED], [REDACTED]'s supervisor at the time. [REDACTED], who has moved [REDACTED], did not return repeated telephone voicemails from the OIG. DOJ declined prosecution.

OIG Disposition:

The OIG issued a Report of Investigation (ROI) to the Commission and FEC management on February 24, 2011. In the ROI, the OIG found that based on the available evidence, the allegations were not substantiated. The ROI recommended no further action concerning [REDACTED], and also recommended that the DAEO train all FEC employees in the recently published revised Standards of Conduct. No further investigative activity is required. Therefore, this investigation is closed.

Concurrence: _____
Jon Hatfield, Deputy Inspector General

_____ Date

**FEDERAL ELECTION COMMISSION
OFFICE OF INSPECTOR GENERAL**



Report of Investigation

Alleged Ethics Violation

Case Number INV-11-01

December 29, 2011

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

<u>Table of Contents</u>		<u>Page</u>
I.	Executive Summary	1
II.	Allegation	2
	<p>██████████ may have violated 18 U.S.C. §§ 203 and 205, prohibiting government employees from representing third parties before the Federal government and receiving compensation for such representation, and 5 C.F.R. § 2635.805, prohibiting Federal employees from testifying as expert witnesses in cases where the Federal government has an interest</p>	
III.	Background	2
	A. Relevant Statutes, Regulations and Policies	2
	B. Scope of the Investigation	4
IV.	Investigation Details	4
V.	Findings	7
VI.	Recommendations	7
VII.	Privacy Act and Freedom of Information Act Notice	8
	Attachment List	9

I. Executive Summary

On September 1, 2011, the Office of Inspector General (OIG) received a hotline complaint in the form of a written referral from [REDACTED] [REDACTED] for the Federal Election Commission (FEC) and [REDACTED] [REDACTED] pursuant to the *Memorandum of Understanding Between the [DAEO] and the Inspector General Concerning the Handling of Ethics Violations*, dated March 13, 1996 (MOU). According to the referral, [REDACTED], an [REDACTED] in the [REDACTED], met with [REDACTED] [REDACTED] and told [REDACTED] that [REDACTED] had represented private clients in Internal Revenue Service (IRS) audits and served as an expert witness. This meeting happened prior to [REDACTED] from the FEC on [REDACTED]. An investigation was opened pursuant to the OIG's *Guidelines for Evaluating OIG Hotline Complaints*.

The referral stated that [REDACTED] may have violated 18 U.S.C. §§ 203 and 205, which generally prohibit government employees from representing third parties before the Federal government. However, the Office of Government Ethics (OGE), in Informal Advisory Opinion 00 x 11, stated representation for the purposes of 18 U.S.C. § 205 does not take place if a government employee appears before the IRS for an audit and only answers factual questions, as opposed to "arguing theories or positions as a way of explaining how or why various decisions were made in preparing the return."¹ 5 C.F.R. § 2635.805 prohibits Federal employees from testifying as expert witnesses in cases where the Federal government has a direct and substantial interest.

[REDACTED] was interviewed by the OIG and stated that he operated a side tax preparation and accounting business for private individual and business clients. [REDACTED] claimed [REDACTED] only appeared before the IRS once in relation to an audit of one of [REDACTED] private clients, and only in the capacity to answer factual questions, and that [REDACTED] never testified as an expert witness. [REDACTED] did not return repeated voicemails left by the OIG in an attempt to obtain additional details, if any, about the matter. [REDACTED] stated the only information [REDACTED] had on this matter was contained in a draft form of the referral that [REDACTED] had left for [REDACTED] before [REDACTED].

FEC Standards of Conduct in place during the time of the alleged violations required employees to seek approval from the Staff Director for any outside employment. However, the FEC Standards of Conduct had been published in 1984 and were rendered unenforceable by subsequent OGE regulations that affected federal agency ethics regulations promulgated prior to 1993. Regardless of whether the FEC Standards of Conduct were enforceable at the time of the alleged violations, [REDACTED] s supervisor, but not the Staff Director per the FEC Standards, had prior knowledge of his outside employment dating to [REDACTED] s hiring.

¹ A person who relies on a formal advisory opinion issued by OGE and acts in good faith is not subject to prosecution or adverse administrative action. 5 C.F.R. § 2638.309(b). OGE Government Ethics Specialist Ryan Segrist confirmed that OGE no longer differentiates between formal and informal advisory opinions, and all advisory opinions are now considered formal.

The OIG investigation did not substantiate the allegations. Therefore, the United States Attorney's Office for the District of Columbia (USAO) declined to prosecute and stated that based on the available evidence, there did not appear to be a criminal violation related to this matter. There is no currently available evidence to support the allegation that [REDACTED], other than the one time to which [REDACTED] admitted, appeared on behalf of or represented any client before the IRS concerning an audit, or that [REDACTED] ever testified as an expert witness. Based on this finding, no further action is recommended concerning [REDACTED]. On a broader scale, it is recommended that the FEC DAEO develop and provide training to all FEC employees on the recently revised FEC Standards of Conduct.

II. Allegation

The OIG investigated the ethics referral that [REDACTED] may have violated 18 U.S.C. §§ 203 and 205, which generally prohibit government employees from representing third parties before the Federal government and receiving compensation for such representation, by representing private clients during IRS audits. The OIG also investigated the allegation that [REDACTED] may have violated 5 C.F.R. § 2635.805, which prohibits Federal employees from testifying as expert witnesses in cases where the Federal government has a direct and substantial interest, by testifying as an expert [REDACTED] in tax and fraud litigation. Evidence obtained during the investigation indicates that [REDACTED] conducted a side tax preparation and accounting business for both individual and business clients, that [REDACTED]'s supervisor knew of [REDACTED] side business, and that [REDACTED] at least once appeared before the IRS to answer factual questions relating to the preparation of a tax return for one of [REDACTED] clients, while at the same time employed by the FEC. However, the OIG was unable to substantiate the allegations of a violation of any criminal law or regulation.

III. Background

A. Relevant Statutes, Regulations and Policies

It is a crime under 18 U.S.C. § 203(a) for anyone who is an officer or employee of the United States government, other than in the discharge of their official duties, to demand[], seek[], receive[], accept[], or agree[] to receive or accept any compensation for any representational services, as agent or attorney or otherwise, rendered or to be rendered either personally or by another . . . in relation to any proceeding, application, request for a ruling or other determination, contract, claim, controversy, charge, accusation, arrest, or other particular matter in which the United States is a party or has a direct and substantial interest, before any department, agency, court, court-martial, officer, or any civil, military, or naval commission.

It is a crime under 18 U.S.C. § 205(a)(2) for anyone who is an officer or employee of the United States government, other than in the discharge of their official duties, to “act[] as agent or attorney for anyone before any department, agency, court, court-martial, officer, or civil, military, or naval commission in connection with any covered matter in which the United States is a party or has a direct and substantial interest.” A “covered matter” includes “any judicial or other proceeding, application, request for a ruling or other determination, contract, claim, controversy, investigation, charge, accusation, arrest, or other particular matter.” 18 U.S.C. § 205(h).

In interpreting these statutes, OGE has opined that the mere preparation of another’s tax return, signing another’s tax return as a preparer or “the provision of purely factual information” does not violate 18 U.S.C. § 203. OGE Informal Advisory Opinion 89 x 7 (*citing* OGE Informal Advisory Opinions 86 x 9, 85 x 3, 81 x 21). OGE Informal Advisory Opinion 00 x 11 states representation for the purposes of 18 U.S.C. § 205 does not take place if a government employee appears at an IRS audit and only answers factual questions, but “arguing theories or positions as a way of explaining how or why various decisions were made in preparing the return” could result in a violation. Further, a government employee “may not attempt to correct any erroneous information in the file or discuss any matter that is an actual or potential controversy.” OGE Informal Advisory Opinion 00 x 11.

5 C.F.R. § 2635.805(a) prohibits Federal employees from testifying as an expert witness “in any proceeding before a court or agency of the United States in which the United States is a party or has a direct and substantial interest.”

FEC Standards of Conduct found in 11 C.F.R. § 7.9, as promulgated on September 29, 1986, and ostensibly in effect at the time of the alleged violations, prohibited FEC employees from devoting a substantial amount of their time to “any other business, vocation or employment,” and from engaging in outside employment that would be incompatible with the discharge of their official duties, result in a violation of law or regulation, or result in a real or perceived conflict of interest or “conflict between their private interests and official duties.” 11 C.F.R. § 7.9(a), (b)(1) – (3), (5). FEC employees were also required to obtain approval for outside employment from the General Counsel or Staff Director, as well as the DAEO. *Id.* at (f). However, 11 C.F.R. § 7.9 was superseded by Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635, and rendered unenforceable by 5 C.F.R. §§ 2635.105 and 2635.803; these regulations required agency supplemental regulations concerning prior approval for outside employment and activities to receive concurrence and be jointly issued by OGE after February 3, 1993. Revised FEC Standards of Conduct which are in compliance with 5 C.F.R. 2635.105 became effective on December 14, 2011.

B. Scope of the Investigation

The OIG received the ethics referral on September 1, 2011, and Hotline complaint number HL-11-02 was assigned. The formal investigation was opened on the same day. The OIG interviewed [REDACTED]; [REDACTED]; [REDACTED]'s supervisor; and received additional information from [REDACTED]. At the beginning of his October 26, 2011, interview, [REDACTED] was provided a Garrity warning and was notified of [REDACTED] Weingarten rights, and [REDACTED] signed the written acknowledgements.

IV. Investigation Details

This matter was initiated on September 1, 2011, when the OIG received a written referral from [REDACTED] pursuant to the MOU. (Attachment 1). The referral states that [REDACTED] initiated a meeting with [REDACTED] because a friend of [REDACTED]'s had told [REDACTED] [REDACTED] might be engaging in prohibited activities. This meeting happened sometime prior to [REDACTED] from the FEC on [REDACTED], but there is no independent evidence of the exact date. According to the referral, [REDACTED] told [REDACTED] that [REDACTED] had been preparing tax forms for private clients for the past ten (10) years, and that he had represented "some" private clients in IRS audits and testified as a [REDACTED] expert witness in tax and fraud litigation. The referral states [REDACTED] told [REDACTED] "the activities were potentially illegal, and that [REDACTED] should discontinue any such activity beyond the preparation of tax forms." The referral contains no other information as to the substance of the conversation between [REDACTED] and [REDACTED] or concerning the specifics of [REDACTED]'s alleged representation of private clients at IRS audits and service as an expert witness. According to [REDACTED], the only information left by [REDACTED] concerning this matter was a rough draft of the referral to the OIG. A search of the ethics files pursuant to an OIG request revealed no additional information.

The referral states that [REDACTED] attended session one (1) of "Ethics Survivor" training (Survivor training), which was presented in the format of a game modeled on the television show *Survivor*, on [REDACTED]. Line fourteen (14) of the sign-up sheet for the Survivor training shows [REDACTED]'s printed first and last name and initials. (Attachment 2). The Ethics Training Attendance 2009 sheet lists [REDACTED] as attending session one (1) of the Survivor training. (Attachment 3). PowerPoint slide 19 of the Survivor training asks the question, "For 400 points: Which of the following is an impermissible representational activity?" (Attachment 4) (Emphasis in original). Slide 20 of the Survivor training reveals the answer to be "c. Representing your uncle at his IRS audit." (Attachment 4).

On October 26, 2011, Deputy Inspector General Jon HATFIELD and Chief Investigator J. Cameron THURBER interviewed [REDACTED]. Prior to the interview, [REDACTED] was advised of his Garrity rights and given an Employee Rights (Union Representative/Weingarten) notification;

██████████ signed both acknowledgement forms. ██████████ voluntarily participated in the interview and provided the following statements:

- ██████████ has worked at the FEC as ██████████ since ██████████. As ██████████ ██████████ work primarily consists of ██████████, and does not involve any tax-related work. ██████████ has a home-based side business focusing on business and personal income tax work, but it does not involve any of the same skill sets or knowledge as ██████████ work as ██████████. ██████████ has never done work for private clients on FEC time, and has never used FEC resources for ██████████ side business. ██████████ has had this side business since before becoming employed with the FEC, and during ██████████ FEC employment interview revealed that ██████████ did this work and intended to keep doing it while employed by the FEC. It is common knowledge in ██████████ that ██████████ does this work.
- Most of ██████████'s clients are individuals, and the rest are business clients. ██████████ provides tax advice to ██████████ clients, and prepares and signs income tax returns. At one point, ██████████ had approximately four hundred (400) clients, but ██████████ now has approximately half that many.
- ██████████ has never used ██████████ position with the FEC to attempt to recruit clients, and ██████████ does not believe ██████████ clients generally know of ██████████ work with the FEC because ██████████ usually does not mention it; however, ██████████ believes ██████████ told some clients about ██████████ FEC position. ██████████ helps ██████████ with the ██████████ but does not charge ██████████.
- ██████████ only assisted one client in an IRS audit about three (3) or four (4) years ago.² The IRS tax return in question was from 2007, and the audit took place in 2008. After ██████████ FEC working hours, ██████████ met with the IRS agent and the client two (2) or three (3) times at ██████████ client's place of business over a course of approximately six (6) months. The client could not explain an issue concerning a tax return, so the IRS agent called ██████████. ██████████ provided ██████████ work papers to the IRS agent and answered factual questions from the agent. ██████████ said ██████████ did not provide any new information after the first meeting, but would go over the same information at each meeting. ██████████ "only answered what was asked" by the IRS agent and did not try to advance ██████████ client's interests.
- All of the questions ██████████ answered for the IRS agent concerned line 17 (income from rent) on his client's Form 1040. ██████████ "merged" the amount on line 17 from two other documents, the client's Schedule E and a Form K-1, and placed the

² ██████████ contends that ██████████ did not "represent" the client, as ██████████ only answered questions and provided factual information in the course of the audit.

combined amount on line 17. The fact that the client also had an S-corporation also figured into the tax return preparation. [REDACTED] does not retain the documentation [REDACTED] clients provide for the tax returns, and the client was unable to produce the documentation for part of the amount. Ultimately, the IRS disallowed part of the amount and made the client recalculate what [REDACTED] owed. The IRS sent the client a bill, but the client did not have to file an amended return.

- [REDACTED] has never served as an expert witness in any federal or state court case, although he has been asked to do so once or twice.
- [REDACTED] attended the Survivor training, which was facilitated by [REDACTED]. [REDACTED] was shown a sign-in sheet from the training, dated [REDACTED] 2009, from [REDACTED], and he confirmed his handwritten name and initials on line 14. [REDACTED] said the training "hit me hard," and [REDACTED] decided to speak with [REDACTED] soon after the training. [REDACTED] does not remember what part of the training "hit [REDACTED] hard," but [REDACTED] was shown slides 19 and 20 of the Survivor training (discussed supra), and said that it could have been that part.
- [REDACTED] believes he called [REDACTED] "right after the [Survivor] training," although [REDACTED] is not sure how soon after, and asked to meet with [REDACTED]. [REDACTED] met with [REDACTED] in [REDACTED]'s office for approximately thirty (30) minutes. [REDACTED] told [REDACTED] that [REDACTED] was a part-time [REDACTED] and did work giving advice concerning and preparing tax returns for individual and business clients. [REDACTED] told [REDACTED] that [REDACTED] was "helping" a client in an IRS audit and that it involved line 17 on a Form 1040, but did not go into much further detail about the assistance. [REDACTED] told [REDACTED] [REDACTED] was sorry if [REDACTED] had done anything wrong. [REDACTED] told [REDACTED] "don't do this" again, told [REDACTED] could not represent clients before the IRS, and advised [REDACTED] to stop all representational activity. [REDACTED] believes that when [REDACTED] said "this," it meant contact with the IRS. [REDACTED] asked [REDACTED] if [REDACTED] ever worked as an expert witness, and [REDACTED] stated, "Never."

Several attempts to contact [REDACTED], who apparently moved to the [REDACTED] area following [REDACTED], were made using his last known contact information, but to no avail.

On October 28, 2011, THURBER interviewed [REDACTED], who stated the following:

- [REDACTED] was [REDACTED]'s supervisor from when [REDACTED] first started at the FEC until [REDACTED] was [REDACTED]. [REDACTED] was aware that [REDACTED] worked during [REDACTED] off hours giving tax advice and "doing tax work" for private tax clients. Other FEC employees were aware of [REDACTED]'s private tax work, including [REDACTED] and most of the staff [REDACTED] of the FEC building. [REDACTED] never asked permission to work during

off hours for private clients, but it was understood between [redacted] and [redacted] that [redacted] was doing this.

- [redacted]'s current supervisor is [redacted]. [redacted] believes that [redacted] is aware of [redacted]'s private client tax work, and [redacted] vaguely recalls mentioning the work to [redacted] during [redacted].
- [redacted]'s private tax work never interfered with his FEC position or work performance. [redacted] was not aware of [redacted] ever using FEC resources for [redacted] private tax clients.

THURBER briefed Assistant United States Attorney Steve DURHAM, Chief of the Public Corruption Unit at the USAO, on the ethics complaint prior to [redacted]'s interview. Following [redacted]'s interview, [redacted]'s interview, and the failed attempts to contact [redacted], THURBER again briefed DURHAM on case developments, and DURHAM declined prosecution on behalf of the USAO.

V. Findings

The OIG investigation made the following findings:

- Due to the lack of direct evidence, the OIG was unable to substantiate the allegation that [redacted] violated 18 U.S.C. §§ 203 or 205, which generally prohibit government employees from representing third parties before the Federal government and receiving compensation for such representation, by representing private clients during IRS audits, and 5 C.F.R. § 2635.805, which prohibits Federal employees from testifying as expert witnesses in cases where the Federal government has a direct and substantial interest, by testifying as an expert [redacted] witness in tax and fraud litigation.
- Based on an interview with [redacted], [redacted]'s private tax work did not interfere with [redacted]'s FEC position or work performance at the time of the alleged violations.

VI. Recommendations

Based on these findings, the OIG recommends that management consider the following:

- No further action is recommended concerning [redacted].

- The FEC DAEO, through and in cooperation with FEC management, should develop and provide training to all FEC employees on the revised FEC Standards of Conduct, published in 76 Fed. Reg. 70322 (Nov. 14, 2011), with an effective date of December 14, 2011.
- The FEC DAEO should provide a response to the Inspector General within 60 days of this report documenting their training plan(s) or status of the recommendation contained in this report. The training should be provided during the next scheduled annual ethics training cycle, and the FEC DAEO should provide a follow-up response once this training has been completed.

VII. Privacy Act and Freedom of Information Act Notice

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. §552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENTS

Attachment	Description
1	Referral from DAEO, dated September 1, 2011
2	Survivor training sign-up sheet, dated July 9, 2009
3	Ethics Training (Survivor) Attendance 2009 sheet, dated July 9, 2009
4	Ethics Survivor training PowerPoint slides 1, 19 and 20

Attachment No. 1

Referral from DAEO,
dated September 1, 2011

Case Number INV-11-01

THE OFFICE OF
INSPECTOR GENERAL

2011 SEP -1 PM 2:43



FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

September 1, 2011

CONFIDENTIAL MEMORANDUM

TO: Lynne A. McFarland
Inspector General

FROM: [Redacted]
Designated Agency Ethics Official

[Redacted]
Alternative Designated Agency Ethics Official

RE: Referral of [Redacted]

We are referring to your office a "possible ethics violation" as provided for in the Memorandum of Understanding between the Designated Agency Ethics Official and the Inspector General. The information herein is based on a conversation between [Redacted] and [Redacted] Deputy Ethics Official [Redacted] prior to [Redacted] from the agency.

[Redacted] is employed as [Redacted] within the [Redacted] of the Commission's [Redacted]. In a meeting with [Redacted] held at [Redacted] request, [Redacted] told [Redacted] that for the past [Redacted] years he had been preparing taxes for private clients. [Redacted] stated that during that time, [Redacted] had represented some of [Redacted] private clients in audits before the IRS, and had also served as an expert witness providing [Redacted] in tax or fraud litigation.

[Redacted] stated that [Redacted] was seeking ethics advice because a friend had told [Redacted] that as a federal employee [Redacted] might be prohibited from engaging in these activities. [Redacted] stated that [Redacted] had never informed any of [Redacted] clients that [Redacted] was a federal employee, and that [Redacted] kept [Redacted] business activities completely separate from [Redacted] work at the FEC.

[Redacted] instructed [Redacted] that the activities were potentially illegal, and that [Redacted] should discontinue any such activity beyond the preparation of tax forms.

Memorandum to Lynne McFarland
Page 2

The activity [REDACTED] described implicates 18 U.S.C. §§ 203 and 205. Section 205 is a criminal statute that prohibits federal employees (except under certain circumstances not relevant here) from representing private clients before the Federal Government. It is a representational bar, applying to an appearance before the government on behalf of another to request action or argue a position in a matter of controversy. Section 203 prohibits Federal employees from receiving compensation for the representation of private clients before the Federal Government.

In addition, 5 C.F.R. § 2635.805, a regulation of the Office of Government Ethics, prohibits federal employees from serving, without authorization from their employing agency, as an expert witness testifying on behalf of a private party in any case in which the Federal Government has a direct and substantial interest.

Please note that the Office of Government Ethics has consistently stated in informal Advisory Opinions that the mere preparation of someone else's income taxes, or even the signing of someone else's returns as the preparer, does not violate 18 U.S.C. §§ 203 or 205. See, e.g., OGE Informal Advisory Opinion 89 x 7. However, appearance with a client at an IRS audit may or may not violate Section 205, depending on the circumstances. As OGE advised a federal employee in Informal Advisory Opinion 00 x 11:

While you may attend the audit and answer direct factual questions, you may not argue any theories or positions as a way of explaining how or why various decisions were made in preparing the return. The latter would be prohibited by Section 205, because you would then be representing the taxpayer in the audit.

Similarly, while the expert witness regulation at 5 C.F.R. § 2635.805 would clearly prohibit a federal employee from giving record testimony as an expert in a case before a court or an administrative tribunal in which the Federal Government had a direct and substantial interest, it is not clear that it would go farther to prohibit an employee from conducting [REDACTED] as a hired expert or consultant on behalf of a private party in connection with litigation if no testimony by the federal employee was involved.

We have no information that [REDACTED] explored with [REDACTED] the specifics of any appearance [REDACTED] may have made at a private client's audit, or the details of [REDACTED] work as "an expert witness doing [REDACTED]"

Our records do indicate that [REDACTED] attended a session of the "Survivor" live ethics training provided to all Commission employees in 2009. Of note, the example of impermissible representational activity that was used in that training was representation of a private party in an IRS audit.

Our records do not indicate whether or not [REDACTED] received specific ethics training on this issue prior to 2009. [REDACTED] position at the Commission is not one for which the filing of a financial disclosure report is required. [REDACTED] has previously sought ethics advice on outside employment, but the proposed employment in that instance involved teaching, not

Memorandum to Lynne McFarland
Page 3

representational activities, and thus there was no occasion in that guidance to discuss the statutes applicable to such activities.

Please feel free to contact [REDACTED] if you seek additional information.

Attachment No. 2

Survivor training sign-up sheet,
dated July 9, 2009

Case Number INV-11-01

Attachment No. 3

**Ethics Training (Survivor) Attendance 2009 sheet,
dated [REDACTED] 2009.**

Case Number INV-11-01

Attachment No. 4

Ethics Survivor training PowerPoint slides 1, 19 and 20

Case Number INV-11-01

ETHICS SURVIVOR

8) For 400 Points:

Which of the following is an impermissible representational activity?

- a. Serving as a character witness for a friend being prosecuted for a federal crime
- b. Representing, w/out pay, a friend with whom you used to work at EPA at an EPA disciplinary hearing
- c. Representing your uncle at his IRS audit
- d. In your capacity as trustee, representing the beneficiaries of the trust on a matter involving the trust

8) For 400 Points:

Which of the following is an impermissible representational activity?

- a. Serving as a character witness for a friend being prosecuted for a federal crime
- b. Representing, w/out pay, a friend with whom you used to work at EPA at an EPA disciplinary hearing
- c. **Representing your uncle at his IRS audit**
- d. In your capacity as trustee, representing the beneficiaries of the trust, on a matter involving the trust

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.



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

CASE CLOSING MEMORANDUM

Case #: INV-13-04	Prepared By: J. C. Thurber
Case Title: Hatch Act Referral	
Date of Report: July 2, 2014	
Subject: [REDACTED]	

Hotline Complaint HL-13-09 was opened on November 1, 2013, following the Office of Inspector General's (OIG) receipt of a referral from the [REDACTED] to the Office of Special Counsel (OSC). The referral alleged that [REDACTED], an attorney in the [REDACTED], had violated the Hatch Act through [REDACTED] political activity on Twitter. INV-13-04 was opened the same day, in accordance with OIG Hotline Complaint evaluation guidelines.

A joint investigation was initiated with the OSC. During the course of the investigation, the OIG learned that [REDACTED] had also appeared on a live webcast discussing the presidential election that was broadcast from the FEC building. [REDACTED] resigned from the FEC on April 5, 2014, pursuant to a settlement agreement she reached with the OSC. [REDACTED] admitted to violating the Hatch Act, as well as conducting political activity while on duty and from the FEC building. DOJ was contacted and declined prosecution.

OIG Disposition:

The OIG issued a Report of Investigation (ROI) to the Commission and FEC management on June 25, 2014. In the ROI, the OIG found that [REDACTED] had misused government property and official time, and had violated the agency's supplemental ethics regulations. The ROI recommended the agency consider revising the supplemental ethics regulations and issuing a directive to strengthen the prohibitions on political conduct. No further investigative activity is required. Therefore, this investigation is closed.

Concurrence: _____

Lyune A. McFarland, Inspector General

Date _____



FEDERAL ELECTION COMMISSION

WASHINGTON, D.C. 20463

Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Lynne A. McFarland *LAM*
Inspector General

SUBJECT: Investigation into Hatch Act-related Violations
Case Number: INV-13-04

DATE: June 25, 2014

This memorandum transmits the Office of Inspector General's (OIG) Report of Investigation for case number INV-13-04, which is dated June 24, 2014.

On November 1, 2013, the Federal Election Commission (FEC) Office of General Counsel (OGC) notified the OIG that it had made a referral to the Office of Special Counsel (OSC) concerning [REDACTED] attorney [REDACTED] [REDACTED] had sent several tweets that appeared to violate the Hatch Act, as they expressed support and solicited contributions for the election of candidates for Federal office. [REDACTED] was also found to have used FEC property during [REDACTED] work day to make public comments regarding the 2012 presidential election as a panelist on a national media webcast.

The OIG initiated a joint investigation with the OSC's Hatch Act Unit. The OSC investigated the alleged Hatch Act violations, and the OIG investigated the potential criminal, ethics, and administrative violations, including misuse of government property and misuse of official time. Due to potential criminal violations, the Office of the United States Attorney for the District of Columbia (USAO) was notified.

During the investigation, [REDACTED] entered into a settlement agreement with the OSC, and resigned from the FEC, as required by the agreement's terms, effective April 5, 2014. The USAO issued a declination of prosecution on June 3, 2014. Based on the results of the investigation, the OIG recommends that the Commission consider promulgating a directive to explicitly address using FEC property for political purposes and revising its supplemental ethics regulation to specifically address the outside activity of public political commentary. These recommendations are detailed in the Recommendations section of the report of investigation.

Should you have any questions, please contact my office at 202-694-1015. Thank you.

cc: Lisa J. Stevenson, Deputy General Counsel for Law
Gregory R. Baker, Deputy General Counsel for Administration

From: FOIA@fec.gov
Date: Aug 1, 2016 5:34:08 PM
Subject: Your Freedom of Information Act Request to the Federal Election Commission
-- Document Production 2 (FOIA 2016-32)

VIA ELECTRONIC MAIL

Re: Your FOIA Request to the Federal Election Commission, 2016-32

This letter serves as the Federal Election Commission's (FEC) second document production and final response to your request for information from the FEC under the Freedom of Information Act (FOIA), dated February 29, 2016 and received by the FEC's FOIA Requester Service Center the same day. You requested the following:

Copies of the final report, report of investigation, closing memo, referral memo, referral letter, and "any other conclusory" documents associated with the following closed Office of the Inspector General (OIG) investigations:

INV-08-01	INV-10-02	INV-13-04
INV-08-02	INV-11-01	INV-14-01
INV-09-01	INV-13-01	INV-14-02
INV-09-02	INV-13-02	INV-15-01
INV-10-01	INV-13-03	INV-15-02

On May 11, 2016, the FOIA Requester Service Center sent the Agency's response letter and first document production for your request. With this letter we are releasing the remaining non-exempt documents responsive to your request. See attached. As indicated in our May 11, 2016 letter, the Agency was unable to locate any responsive records related to INV-08-02; and the FEC does not responsive records related to INV-13-01, INV-13-02, INV-13-03, INV-14-01, INV-14-02, INV-15-01, and INV-15-02, as these investigations are not closed.

From the attached documents we have redacted certain information pursuant to FOIA Exemptions 3(A), 4, 6, 7(C), and 7(D). Exemption 3(A) prevents disclosure of information "specifically exempted from disclosure by statute (other than section 552b of this title), if that statute — (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3)(A). Pursuant to Section 7 of the Inspector General Act of 1978, the FEC is prohibited from disclosing the identity of an employee without the consent of the employee, after receipt of a complaint. 5 U.S.C. app. § 7(b). Exemption 4 protects from disclosure trade secrets and other confidential business information. 5 U.S.C. § 552(b)(4). Exemption 6 protects from disclosure information that if released would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6). Exemption 7(C) protects from disclosure records or information compiled for law enforcement purposes that, if released, could reasonably be expected to constitute an

unwarranted invasion of personal privacy. 5 U.S.C § 552(b)(7)(C). Exemption 7(D) provides protection for “records or information compiled for law enforcement purposes [which] could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.” 5 U.S.C. § 552(b)(7)(D).

Some documents related to INV-09-02 contained information of interest to the Federal Communications Commission (FCC). As such, the FEC referred these pages to the FCC’s FOIA Office for FOIA consultation. The FEC has received a response from FCC’s FOIA Office as to the consultation request and those pages are included in the attached documents. The FCC has asserted FOIA Exemption 6 as to certain information in the documents. The pages containing redactions made per the FCC contain the following header: “Per the FCC, Redactions Pursuant to FOIA Exemption 6.” You may appeal any adverse FOIA determination as it relates to the FCC’s redactions by writing to the following address within 30 calendar days of the date of this written decision:

Federal Communications Commission
445 12th Street, S.W.
Room 1-A836
Washington, DC 20554

We have withheld from disclosure approximately 23 pages of responsive documents pursuant to FOIA Exemptions 3(A), 6, 7(C), and 7(D). Additionally, approximately 107 pages of responsive documents have been withheld from disclosure pursuant to FOIA Exemptions 6 and 7(C).

You may appeal any adverse FOIA determination. Any such appeal must be filed in writing and should follow the guidelines set forth in 11 C.F.R. § 4.8. If you have any questions, please contact the FOIA Requester Service Center at FOIA@fec.gov, or (202) 694-1650. Thank you for contacting the FEC.

Sincerely,

Peter Han
FOIA Requester Service Center

Attachment No. 1

FEC Commission Directive No. 54
effective August 15, 2001.

Case Number INV-09-01

FEDERAL ELECTION COMMISSION		
MANUAL OF DIRECTIVES	COMMISSION DIRECTIVE	
	REVOKES March 17, 1992	NO. 54
	EFFECTIVE DATE: August 15, 2001	
Employee Transit Benefit Program		

I. Policy

1. The Federal Election Commission (FEC) promotes and endorses programs that encourage employees to commute to and/or from work by means other than single-occupant vehicles. To achieve this, financial incentives of up to the Federal tax-excludable amount or the actual commute cost, whichever is less, may be provided to employees who regularly commute via public transportation.
2. Cash reimbursement shall not be used. Fare media such as Metrocheks or another form of transit pass will be used for direct distribution to employees.
3. FEC personnel who commute to the FEC, on a regular and recurring basis, on public transportation are eligible to participate in the program. Employees who commute in a private carpool or who receive a Federal parking benefit may not participate in the transit benefit program. A Federal parking benefit provides an employee with vehicle parking at a cost lower than local prevailing commercial parking rates.
4. FEC transit subsidy is to be used for the commute to and/or from the official duty station. The official duty station for all FEC employees is 999 E Street, NW, Washington, DC, other designated leased office space in the Washington, DC metro area or temporary local duty station. Giving or selling FEC-subsidized Metrocheks to others, or knowingly purchasing FEC-subsidized fare media from another, is prohibited.

II. References:

1. Title 26, USC, Section 132(f), the Energy Policy Act of 1992,
2. Federal Employees Clean Air Incentives Act of 1993,
3. Transportation Equity Act of the 21st Century (1998),
3. OMB Circular A-11 Prep and Submit Budget Estimates,
4. OPM Decision Letter S001842 of August 11, 1998,

5. IRS Notice of Proposed Rulemaking Jan 27, 2000, and
6. Executive Order 13150.
7. www.wmata.com/metrochek/metrochek_process.htm. This web site provides guidance on how to exchange your unused Metrochek for fare of equal or greater value for other participating transit services in the area.
8. www.wmata.com/metrochek/metrochek_participants.htm. This web site provides a list of Metrochek participants in the MD, VA, DC area.

III. Action

This Administrative Directive amends the FEC transit benefit program put into effect in April 1992.

IV. Program Eligibility

1. Eligible employees include: any person on a full-time or part-time work schedule who is listed on the FEC payroll, including summer hires, students, law clerks, legal interns, term employees, and temporary employees. FEC employees on an intermittent schedule are not eligible for the program. Any person detailed to, or working at FEC, who is on the payroll of another agency or company, and not the FEC, may not participate in the program.
2. FEC staff who will not be commuting to the FEC for a month or more as a result of extended travel (e.g., out-of-town audit or training) or annual or sick leave (e.g., maternity leave) may not receive fare media for the period of absence from the FEC.
3. The purpose of the FEC transit subsidy program is to provide financial incentives to employees who regularly commute via public transportation. For the purposes of this program, "regularly commute" shall mean that the employee commutes via public transportation on a regular and recurring basis and that a minimum of 50% of the available number of commuting days (business days) per month between home and the official duty station are on public transportation.

Examples of eligibility:

- a. Mr. Doe works full time 5 days a week, taking public transportation both to and from work on an average of 20 work days (or 40 one-way trips) per month. Since Mr. Doe takes public transportation to and from work over 50% of the time, he is eligible to participate in the FEC Transit Subsidy program.
- b. Ms. Jones rides to work with Mrs. Doe most of the time, and uses public transportation only occasionally (less than 50% of the business days per month). Ms. Jones is not eligible for a transit benefit because her use of public transportation is not regular and recurring.

c. Mr. Davis rides in a carpool that parks in the FEC garage using an FEC-issued parking pass. Ms. Peterson rides in a carpool with neighbors that does not park in the FEC garage and does not have an FEC-issued parking pass. Neither Mr. Davis nor Ms. Peterson is eligible for any transit benefit no matter how many times they may ride Metro when not riding in their carpool.

d. Ms. James regularly commutes to her FEC office using public transportation and is eligible for Transit Subsidy. However, from June through August she is on maternity leave. Ms. James may not collect her transit subsidy until she resumes her regular commute to the FEC in September.

e. Mr. White is a part time employee who works 15 days per month and commutes on public transportation. He is eligible to receive a full transit subsidy because he works more than 50% of the business days each month.

4. Employees participating in non-eligible (private or receiving a Federal parking benefit) car pools/van pools are excluded from the program.

5. Ineligibility is effective immediately once the employee no longer meets the requirements for participation in this directive. Once eligibility is terminated all unused or partially used Metrocheks are to be returned to the Finance Office.

V. Subsidy Amount

1. The amount of transit subsidy provided to an employee may not exceed the maximum allowable rate set by law or the employee's actual cost of using eligible mass transportation or a commuter highway vehicle, rounded up to the nearest transit media amount, whichever is less. Employees' fare media amount is determined by the information obtained on their FEC Transit Subsidy Program Participant Application. The employee's monthly fare media amount is determined by the actual daily commuting costs multiplied by 20-work days. Employees must submit a new Transit Subsidy Program Participant Application if there is a permanent change in their commuting pattern.

2. Alternate Fare Media Calculation. For a variety of reasons, employees may vary their monthly commute to their official duty station and not take public transportation every day. This may occur as a result of annual or sick leave or official travel. When a change in commuting pattern results in the employee commuting less than 50% of the business days in a month, an alternate fare media calculation will apply:

a. Scheduled absence from the official duty station:

When employees know that they will not be commuting to the office using public transportation for 50% or more of the business days in a month, they will be entitled to

50% of their full transit benefit for that month.

Formula: The transit subsidy will be adjusted by issuing the employee one-half of the full transit subsidy, rounded up to the next five dollar increment.

Example: Ben receives \$65 each month, but as a result of a two-week vacation in July, he will **not** commute to work 50% of the business days in the month. Therefore, at the end of June he should only request and receive \$35 in subsidy ($\$65 \times .5 = \32.50 , rounded up to \$35).

b. Unscheduled absence from the official duty station:

If after accepting the full amount of transit subsidy for the monthly commute, an employee does not commute to the official duty station for at least 50% of the commuting (business) days because of unplanned or unscheduled absences from the work site, the employee is eligible for 50% of the full transit benefit the following month.

Example: Joan receives \$65 each month and received the full amount for June, but as a result of unforeseen official travel that occurred in the last two weeks in June, she only commuted to work 50% of the business days in the month. As a result, Joan should request 50% of her full transit amount in July.

3. Employees will elect either the full amount or 50% of the transit benefit when they sign the Transit Subsidy Eligibility List each month. Employees will be given Metrocheks totaling either the full amount of the subsidy or 50% of the amount, depending on the amount they designate on the form. It is the employees' responsibility to designate the correct subsidy amount based on their anticipated use of public transportation the next month or their actual use in the previous month.

VI. Processing Applications:

1. Applications for the transit subsidy are available in the Personnel Office (Attachment 1). Applications received by the 20th of each month will be processed and maintained by the Personnel Office for inclusion in the list of approved applicants to receive transit benefits the following month. Once an application is approved by the Personnel Office, the required application information is used to create the list of employees eligible for the transit subsidy. Once approved, employees remain eligible until they leave the employment of the FEC or their commuting pattern changes in such a manner as to make them no longer eligible.

2. When the list of approved applicants (updated monthly by the Personnel Office) has been provided to the Finance Office each month, the Transit Subsidy Eligibility List is used in distributing Metrocheks. The Finance Office will distribute Metrocheks on the last Thursday and Friday of the month and the following Monday. Additional distribution hours are the next Monday through Friday after the initial three-day period. Exceptions occur around the

Thanksgiving Day and Christmas Day holidays, and the Finance Office will send an e-mail to FEC staff that provides the schedule for the holiday periods. Office hours for pick up are 9:30 a.m. to 11:30 a.m. and 1:30 p.m. to 3:30 p.m. A schedule of pick-up days will be distributed annually. In addition, each month on the day before the beginning of the distribution of the next month's transit subsidy, employees will be reminded by e-mail of the upcoming distribution.

3. The Administrative Officer will maintain a current list of employees who have been issued FEC parking permits, including passengers who commute with the parking permit holders. Employees who participate in an FEC carpool and are issued an FEC parking permit will not be eligible for the transit subsidy program. The Personnel Office will compare the list of parking permit holders and their passengers to the Transit Subsidy Eligibility List to ensure that ineligible employees are not on the transit subsidy list.

VII. Employee Responsibilities

1. Upon initial application to the program or implementation of a new maximum rate, employees must complete the FEC Transit Subsidy Program Participant Application and submit it to the Personnel Office. The Personnel Officer will review the application to determine program eligibility and the amount of transit subsidy the employee is entitled.

2. Employees are responsible for monitoring their use of the fare media under the program regulations and must submit a new application to the Personnel Office when their commuting pattern or commuting cost changes, except in the short-term circumstances describe in V.2. Employees who become ineligible to continue the program will immediately notify the Personnel Officer by electronic mail.

3. Employees must agree to return any unused transit subsidy to the Finance Office on their last day of employment with the Commission. The amounts returned may be used for official local travel by other employees. It is not permissible for employees to receive more transit benefits than they use in a month (other than the rounding up to the next fare media amount or the 10% bonus) or for departing employees to use these funds after their final date of employment at the FEC. Departing employees who have transferred their fare media amount to a SmartCard will return any unspent portion of the issued subsidy to the Finance Office in the form of a Metrochek(s) rounded down to the nearest whole dollar value.

4. Employees are responsible for ensuring program eligibility. Employees will certify program eligibility and compliance each month by signing the Transit Subsidy Eligibility List upon receiving their Metrocheks.

5. If an employee loses his/her fare card, it will not be replaced. The employee must wait until the following month to obtain new Metrocheks.

6. Only the employee is eligible for picking up and signing for his/her individual monthly transit

subsidy. There is one exception for employees in the program who are assigned to temporary local duty stations on each of the distribution dates, and therefore, are unable to pick up the transit subsidy. In these cases, the employees' supervisor or another manager in the employees' office or division may receive, sign for, and distribute the monthly fare media to eligible staff on temporary duty at a local offsite duty station. Each employee upon receipt of the fare media will show the supervisor or manager his/her FEC identification card, indicate the full or 50% transit amount, and sign the certification form that certifies eligibility for the fare media. The original signed certification will be forwarded to the Finance Office to serve as documentation that fare media were properly distributed and will be included in the documentation supporting the monthly reconciliation of the fare media distribution. If, by the monthly reconciliation, the Finance Office has not received the distribution sheet from any office or division that picked up fare media for its employees, the Finance Office will contact the office or division to request the sheet.

7. If employees are unable to pick up their transit subsidy because they are out of the office each day of the regular distribution, the Federal Election Commission Request for Late Distribution of Fare Media, FEC Form 10-42, (Attachment 2) may be submitted for approval by the employee's supervisors and the Staff Director. The employee must document on the form absence from the office for the distribution dates.

8. Failure to comply with program requirements can result in disciplinary action, up to and including removal. The making of a false, fictitious or fraudulent certification may render the maker subject to criminal prosecution under Title 18, United States Code, Section 1001, Civil Penalty Action, providing for administrative recoveries of up to \$5,000 per violation.

VIII. Management Responsibilities

1. The Personnel Director is responsible for the approval/disapproval of all transit subsidy applications.
2. The Administrative Office is responsible for the procurement of all Metrocheks for direct delivery to the Finance Office. The Accounting Officer or designee will designate Metrochek Custodians.
3. The Finance Office will notify the Administrative Officer at least seven working days before distribution dates of the total quantity of Metrocheks to order. Orders shall be based on prior usage, stock on hand, and estimated usage for stock.
4. The Administrative Officer shall prepare a purchase order (PO) for purchase of Metrocheks. The PO shall be based on the request from the Finance Office.
5. The purchase order shall include, among other things, the method by which payment of invoices will be made and the specified hours of delivery to the Finance Office.
6. The Washington Metropolitan Area Transit Authority (Metro) will submit an invoice to the

Finance Office for payment of all Metrocheks. Upon receipt, the Finance Office will check the invoice and complete and sign a receiving report. Upon approval, it will be certified for payment by the Certifying Officer.

7. Metrocheks are distributed to the Custodians by the Accounting Officer or designee. The Custodians will:

- a. Sign for receipt of the Metrocheks, and
- b. Count and verify the type and amount of Metrocheks received, in the presence of the Accounting Officer or the designee.

8. The Custodians will have overall responsibility and be held accountable for taking receipt of Metrocheks, safeguarding, and distributing the Metrocheks. Each Custodian's stock of Metrocheks will be reconciled by the Accounting Officer or designee each month.

9. Any transfer of stock between Custodians will be executed by the Accounting Officer or designee on an as needed basis.

10. Metrocheks will be kept in a locked and secure location. The Custodians will have separate safe drawers with locking devices, in which to maintain and control their stock of Metrocheks. Custodians will not have the use of the inventory of other Custodians, unless stock is transferred in accordance with item 9.

11. The stock will be maintained in a standard government-issued safe with a combination lock. Except in emergency situations, as determined by the Accounting Officer or designee, only the Custodians will have access to their individual drawers.

12. A second key to the drawers will be maintained in a sealed/signed envelope under the control of the Accounting Officer or designee.

13. The Custodians will reconcile monthly their receipt and distribution of Metrocheks with the Accounting Officer, or designee. The reconciliation process will involve:

- a. Attaching the Transit Subsidy Eligibility List, the reconciled FEC report of Audit of Fare Media (FEC Form 10-37B), the Fare Media Transfer Document, and the FEC Request for Late Distribution of Fare Media, and any certification form received from offices or divisions that distributed fare media to their employees assigned to temporary, local duty stations;
- b. The Custodians will count the Metrocheks on hand while observed by the Accounting Officer or designee;
- c. the Accounting Officer or designee will record and verify the Metrocheks on hand, distributed to program participants, transferred between Custodians, and resolve any

differences on the FEC Report of Audit of Fare Media, FEC Form 10-37B.

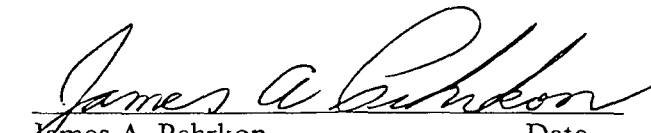
Note: Metrocheks returned to the Custodian as a result of departure from the FEC or determination of ineligibility shall be recorded and maintained separately from the regular inventory and disposed of in the manner allowed by Metro and the Finance Office, including for use by Commission staff for local business travel. The return of Metrocheks to the Finance office will be incorporated into the current Employee Termination Clearance Process.

14. Reported misuse of the Transit Subsidy program by FEC employees will be investigated and the appropriate administrative action will be taken if warranted.

IX. Program Documentation

1. The Personnel Office is responsible for maintaining information about the participants in the program, and the Finance Office is responsible for maintaining information on the distribution of Metrocheks.

Attachments


James A. Pehrkon Date 8/15/01
Staff Director

I certify that I commute to work at the FEC on a regular basis using eligible methods of mass transportation, including Metro Bus or Subway, rail transportation, another bus transportation system, or ride in an eligible van pool. My actual daily and/or monthly commuting costs are depicted below.

I certify that these are the actual, daily costs and methods of my commute based on an average work month of 20 working days. I will notify the FEC if there is any change in the mode or costs of my daily and/or monthly commute to work which could impact on my eligibility to participate in the program or the amount of the subsidy.

Signed: _____

Date: _____

Instructions: Use the applicable daily and monthly cost items to compute your monthly commuting costs. Eligible participants will receive the appropriate monthly subsidy each month, rounded to the next highest \$5 increment, up to the \$65 per month maximum. Eligible van pools are defined as 7 passenger vans (6+ driver), used at over 50% of capacity for 80% or more of the mileage of the daily commute to and from home to work (26 USC 132(f).) Monthly costs are based on either a monthly fare or an average of 20 working days per month (daily rate times 20).

Participants will be required to show FEC ID and certify each month upon receipt of the subsidy that they remain fully eligible to participate and that they are eligible to receive the amount of the subsidy based on actual commuting costs.

COMMUTING COSTS CALCULATIONS FOR TRANSIT SUBSIDY

(USE APPROPRIATE DAILY AND/OR MONTHLY COSTS BOXES TO DEPICT YOUR COSTS PER MONTH)

METRO SUBWAY Daily Costs X 20 Days Monthly Costs
Example: fare each way is \$1.25; daily fare is \$2.50; times 20 days equals \$50 per month.)

METRO BUS Daily Costs X 20 Days Monthly Costs
Example: fare each way is \$1.50; daily fare is \$3.00; times 20 days equals \$60 per month.)

RAIL (VRE/MARC) Daily Costs X 20 Days Monthly Costs
Example: VRE monthly fare is \$165.)

OTHER BUS Daily Costs X 20 Days Monthly Costs
Example: PW Commuteride monthly fare is \$150.)

VAN POOL Daily Costs X 20 Days Monthly Costs
Example: monthly cost of registered, eligible van pool is \$85.)

TOTAL COSTS Daily Costs X 20 Days Monthly Costs

SHORT DESCRIPTION OF MY COMMUTE:

Example: ride VRE each day on monthly ticket of \$165 plus daily commute of \$2.20 on metro subway; total cost of \$209)

NAME: _____
ADDRESS: _____
CITY: _____
STATE: _____

DIVISION _____

PERSONNEL OFFICE USE

ELIGIBLE:

TOTAL COSTS:

TOTAL SUBSIDY:

FEC TRANSIT SUBSIDY PROGRAM--APPLICATION TO PARTICIPATE IN PROGRAM
PART TIME EMPLOYEES

I certify that I commute to work at the FEC on a regular basis using eligible methods of mass transportation, including Metro Bus or Subway, rail transportation, another bus transportation system, or ride in an eligible van pool. My actual daily and/or monthly commuting costs are depicted below.

I certify that these are the actual, daily or monthly costs and methods of my commute based on an average work month of ___ working days. I will notify the FEC if there is any change in the mode or costs of my daily and/or monthly commute to work which could impact on my eligibility to participate in the program or the amount of the subsidy.

Signed: _____

Date: _____

Instructions: Use the applicable daily and monthly cost items to compute your monthly commuting costs. Eligible participants will receive the appropriate monthly subsidy each month, rounded to the next highest \$5 increment, up to the \$65 per month maximum. Eligible van pools are defined as 7 passenger vans (6+ driver), used at over 50% of capacity for 80% or more of the mileage of the daily commute to and from home to work (26 USC 132(f).) Monthly costs are based on either a monthly fare or an average of 20 working days per month (daily rate times 20).

Participants will be required to show FEC ID and certify each month upon receipt of the subsidy that they remain fully eligible to participate and that they are eligible to receive the amount of the subsidy based on actual commuting costs.

COMMUTING COSTS CALCULATIONS FOR TRANSIT SUBSIDY

(USE APPROPRIATE DAILY AND/OR MONTHLY COSTS BOXES TO DEPICT YOUR COSTS PER MONTH)

METRO SUBWAY Daily Costs X ___ Days Monthly Costs
Example: fare each way is \$1.25; daily fare is \$2.50; times 20 days equals \$50 per month.)

METRO BUS Daily Costs X ___ Days Monthly Costs
Example: fare each way is \$1.50; daily fare is \$3.00; times 20 days equals \$60 per month.)

RAIL (VRE/MARC) Daily Costs X ___ Days Monthly Costs
Example: VRE monthly fare is \$165.)

OTHER BUS Daily Costs X ___ Days Monthly Costs
Example: PW Commuteride monthly fare is \$150.)

VAN POOL Daily Costs X ___ Days Monthly Costs
Example: monthly cost of registered, eligible van pool is \$85.)

TOTAL COSTS Daily Costs X ___ Days Monthly Costs

SHORT DESCRIPTION OF MY COMMUTE:

Example: ride VRE each day on monthly ticket of \$165 plus daily commute of \$2.20 on metro subway; total cost of \$20

NAME: _____	PERSONNEL OFFICE USE
ADDRESS: _____	
CITY: _____	
STATE: _____	
DIVISION _____	
	ELIGIBLE: <input type="text" value="YES"/> <input type="text" value="NO"/>
	TOTAL COSTS: <input type="text" value="\$ -"/>
	TOTAL SUBSIDY: <input type="text" value="\$"/>

FEDERAL ELECTION COMMISSION
REQUEST FOR LATE DISTRIBUTION OF FARE MEDIA

NAME FIRST MI

request late distribution of fare media for the month of _____ 20 _____. I was unable to pick-up my fare media on the designated days due to the following reason(s):

Understand that the request has to be made before the end of the month that the fare media represents.

certify that I am eligible for a fare subsidy for use on a participating public transportation systems, and will not transfer it to anyone else.

EMPLOYEE SIGNATURE DATE

Confirmation By:

MANAGER HEAD SIGNATURE DATE

Approved By:

DEPUTY DIRECTOR SIGNATURE DATE

COMMUNAL DIRECTOR SIGNATURE AMOUNT DATE

Forward completed and approved form to the Accounting Office.
The Accounting Office will notify you regarding a distribution time.

Verification that the employee has not received fare media for the above month:

ACCOUNTING OFFICE SIGNATURE DATE

Media Receipt:		No. of Cards	Metrocheck Value
EMPLOYEE SIGNATURE	DATE	_____	\$22.00
		_____	\$10.00
		_____	\$ 5.00

Attachment No. 2

LAZ Parking LTD Records
on FEC employees receiving employee-paid
monthly parking permits
for the months January 2008 – July 2008.

Case Number INV-09-01

Attachment No. 3

FEC Transit Subsidy Program Applications
submitted by 

Case Number INV-09-01

**FEDERAL ELECTION COMMISSION
TRANSIT SUBSIDY PROGRAM APPLICATION**

(Please type or print legibly in blue or black ink)

ACTION REQUESTED (CHECK ONE): New Change Cancellation Annual Recertification Temporary NTE
DATE:

NOTE: Items 1 through 12, and the reverse side of this form must be completed in full before submitting to Human Resources.

APPLICANT INFORMATION

1. NAME OF APPLICANT (Last, First, Middle Initial) [REDACTED]	2. LAST FOUR DIGITS OF SSN [REDACTED]	3. DIVISION [REDACTED]
4. HOME ADDRESS (Street, City, State, Zip Code) [REDACTED]	5. MODE (S) OF TRANSPORTATION TO BE USED DAILY TO COMMUTE TO AND FROM WORK. Bus <input type="checkbox"/> Light Rail <input type="checkbox"/> <input checked="" type="checkbox"/> Subway Ferry <input type="checkbox"/> Train <input type="checkbox"/> Authorized Vanpool <input type="checkbox"/> Other (Specify)	6. TYPE OF FARE MEDIA YOU USE. SmarTrip Card (Card No.) [REDACTED] Fare card <input type="checkbox"/> Tickets <input type="checkbox"/> Pass Tokens <input type="checkbox"/> Voucher <input checked="" type="checkbox"/> SmarTrip Card Other (Specify)
7. WORK TELEPHONE NUMBER [REDACTED]	8. MONTHLY COMMUTING COSTS (from worksheet on back) \$118.00	

EMPLOYEE ACKNOWLEDGEMENT AND CERTIFICATION

- I certify I am employed by the Federal Election Commission.
- I certify I am eligible for a public transportation fare benefit. I will use it for my daily commute to and from work. I will not give, sell, or transfer it to anyone else.
- I certify I am not a member of a carpool. Furthermore, I do not receive disability or executive parking privileges.
- I certify that the monthly transit benefit I receive does not exceed my monthly commuting costs.
- I certify that in any given month, I will not use the Government-provided transit benefit in excess of the statutory limit. If my commuting costs per month exceed the monthly statutory limit, I will supplement those additional costs with my own funds.
- I certify I am responsible for returning unused FEC funded fare subsidy to the Office of Finance no later than my effective date of resignation, transfer, retirement, etc. from the FEC.
- I certify my usual monthly public transportation commuting costs (excluding any parking costs) is the amount listed above (amount is supported by completed worksheet.).
- I understand that I must submit a new Transit Subsidy Program Participant application if there is any permanent change in the information provided above.
- I understand that it is a Federal crime under 18 United States Code, Section 1001, to make a false fictitious or fraudulent statement on this form. If I make a false statement, I may be subject to criminal prosecution and punishment, including a fine and/or administrative punishment, which may result on the termination of my federal employment.

12. DATE

8/7/07

**APPROVED BY THE HUMAN RESOURCES OFFICE
COORDINATOR - HR BENEFIT COORDINATOR**

13. NAME OF HR BENEFIT COORDINATOR	14. AGENCY MAXIMUM BENEFIT (Enter monthly payable amount for each participant based upon commuting costs, statutory limitations, agency policy, Union Negotiations, etc.).
15. SIGNATURE OF HR BENEFIT COORDINATOR	16. DATE
17. ENTERED IN METRO SYSTEM AND FEC DATABASE BY:	18. DATE

PRIVACY ACT STATEMENT

This information is solicited under authority of Public Law 101-509. Furnishing the information on this form is voluntary, but failure to do so may result in disapproval of your request for a public transportation transit fare benefit. The purpose of this information is to facilitate timely processing of your request, to ensure your eligibility, and to prevent misuse of the funds involved. This information will be provided to the Human Resources and Finance to administer this program and to ensure that you are not listed as a carpool participant or a holder of any other form of vehicle work site parking permit with FEC or any other Federal Agency.

CALCULATION OF COMMUTING COST

To be completed by applicant: Use Appropriate Daily and/or Monthly Costs to calculate your costs per month. **Note: Do not include parking costs.**

Mode of Transportation	Daily Costs (round trip)	Multiplied by # of work days (20 for F-T)	Equals Monthly Commute Costs
Subway (METRO)	\$ 5.90	Multiplied by 20 work days	\$ 118.00
Metro Bus	\$	Multiplied by work days	\$
Commuter Train (VRE, MARC, etc.)	\$	Multiplied by work days	\$
Other Bus (e.g., Ride-On)	\$	Multiplied by work days	\$
Van Pool	\$	Multiplied by work days	\$
Other	\$	Multiplied by work days	\$
Total – all costs	\$	Multiplied by work days	\$

Routing Pattern (Required) [REDACTED] to Metro Center and return
Metro Center [REDACTED] and return

Example 1: Vienna to Metro Center and return

Example 2: Line 1 Bus from residence to New Carrollton
 Line 2 Metro to Navy Archive and return. Bus back to residence.

[REDACTED]
08/07/2007 09:29 AM

To [REDACTED]

cc [REDACTED]

bcc [REDACTED]

Subject: Fare Media

[REDACTED]

Please provide [REDACTED] with [REDACTED] fare cards for the month of August in the amount of \$110.00. [REDACTED] commute via the rail from [REDACTED] to Metro Center with a one way rate of \$2.95 and roundtrip \$5.90.

Thanks

NOTE: [REDACTED] has a smartrip card [REDACTED] and will be utilizing [REDACTED] card to download [REDACTED] subsidy as of September 1, 2007.

[REDACTED]
Federal Election Commission
[REDACTED]

How is my customer service? Please complete a brief survey by clicking on the following link.

<http://fecas003.fec.gov/APPS/SurveyQues.nsf/Survey?OpenForm>

Handwritten initials

Recd HR 12/11/07



**FEDERAL ELECTION COMMISSION
TRANSIT SUBSIDY PROGRAM APPLICATION**
(Please type or print legibly in blue or black ink)

ACTION REQUESTED (CHECK ONE): New Change Cancellation Annual Recertification Temporary NTE

DATE: _____

NOTE: Items 1 through 12, and the reverse side of this form must be completed in full before submitting to Human Resources.

APPLICANT INFORMATION

1. NAME OF APPLICANT (Last, First, Middle Initial) [Redacted]	2. LAST FOUR DIGITS OF SSN [Redacted]	3. DIVISION [Redacted]
4. HOME ADDRESS (Street, City, State, Zip Code) [Redacted]	5. MODE(S) OF TRANSPORTATION TO BE USED DAILY TO COMMUTE TO AND FROM WORK. <input type="checkbox"/> Bus <input type="checkbox"/> Light Rail <input checked="" type="checkbox"/> Subway <input type="checkbox"/> Ferry <input type="checkbox"/> Train <input type="checkbox"/> Authorized <input type="checkbox"/> Vanpool <input type="checkbox"/> Other (Specify)	6. TYPE OF FARE MEDIA YOU USE. SmarTrip Card (Card No.) [Redacted] <input type="checkbox"/> Fare card <input type="checkbox"/> Tickets <input type="checkbox"/> Pass <input type="checkbox"/> Tokens <input type="checkbox"/> Voucher <input checked="" type="checkbox"/> SmarTrip Card <input type="checkbox"/> Other (Specify)
7. WORK TELEPHONE NUMBER [Redacted]	8. MONTHLY COMMUTING COSTS (from worksheet on back) \$118.00	

EMPLOYEE ACKNOWLEDGEMENT AND CERTIFICATION

- I certify I am employed by the Federal Election Commission.
- I certify I am eligible for a public transportation fare benefit. I will use it for my daily commute to and from work. I will not give, sell, or transfer it to anyone else.
- I certify I am not a member of a carpool. Furthermore, I do not receive disability or executive parking privileges.
- I certify that the monthly transit benefit I receive does not exceed my monthly commuting costs.
- I certify that in any given month, I will not use the Government-provided transit benefit in excess of the statutory limit. If my commuting costs per month exceed the monthly statutory limit, I will supplement those additional costs with my own funds.
- I certify I am responsible for returning unused FEC funded fare subsidy to the Office of Finance no later than my effective date of resignation, transfer, retirement, etc. from the FEC.
- I certify my usual monthly public transportation commuting costs (excluding any parking costs) is the amount listed above (amount is supported by completed worksheet).
- I understand that I must submit a new Transit Subsidy Program Participant application if there is any permanent change in the information provided above.
- I understand that it is a Federal crime under 18 United States Code, Section 1001, to make a false fictitious or fraudulent statement on this form. If I make a false statement, I may be subject to criminal prosecution and punishment, including a fine and/or administrative punishment, which may result on

[Redacted]	12. DATE 12/11/07
------------	----------------------

**APPROVED BY THE HUMAN RESOURCES OFFICE
COORDINATOR - HR BENEFIT COORDINATOR**

13. NAME OF HR BENEFIT COORDINATOR [Redacted]	14. AGENCY MAXIMUM BENEFIT (Enter monthly payable amount for each participant based upon commuting costs, statutory limitations, agency policy, Union Negotiations, etc.).
15. SIGNATURE OF HR BENEFIT COORDINATOR	16. DATE
17. ENTERED IN METRO SYSTEM AND FEC DATABASE BY:	18. DATE

PRIVACY ACT STATEMENT

This information is solicited under authority of Public Law 101-509. Furnishing the information on this form is voluntary, but failure to do so may result in disapproval of your request for a public transportation transit fare benefit. The purpose of this information is to facilitate timely processing of your request, to ensure your eligibility, and to prevent misuse of the funds involved. This information will be provided to the Human Resources and Finance to administer this program and to ensure that you are not listed as a carpool participant or a holder of any other form of vehicle work site parking permit with FEC or any other Federal Agency.

CALCULATION OF COMMUTING COST

To be completed by applicant: Use Appropriate Daily and/or Monthly Costs to calculate your costs per month. **Note: Do not include parking costs.**

Mode of Transportation	Daily Costs (round trip)	Multiplied by # of work days (20 for F-T)	Equals Monthly Commute Costs
Subway (METRO)	\$ 5.90	Multiplied by 20 work days	\$ 118.00
Metro Bus	\$	Multiplied by work days	\$
Commuter Train (VRE, MARC, etc.)	\$	Multiplied by work days	\$
Other Bus (e.g., Ride-On)	\$	Multiplied by work days	\$
Van Pool	\$	Multiplied by work days	\$
Other	\$	Multiplied by work days	\$
Total - all costs	\$	Multiplied by work days	\$

Routing Pattern (Required) [REDACTED] to Metro Center and return

Metro Center to [REDACTED] and return

Example 1: Vienna to Metro Center and return

Example 2: Line 1 Bus from residence to New Carrollton

Line 2 Metro to Navy Archive and return. Bus back to residence.

**FEDERAL ELECTION COMMISSION
TRANSIT SUBSIDY PROGRAM APPLICATION**

(Please type or print legibly in blue or black ink)

ACTION REQUESTED (CHECK ONE): New Change Cancellation Annual Recertification Temporary NTE

DATE: 2/12/09

NOTE: Items 1 through 12, and the reverse side of this form must be completed in full before submitting to Human Resources.

APPLICANT INFORMATION

1. NAME OF APPLICANT (Last, First, Middle Initial) [REDACTED]	2. LAST FOUR DIGITS OF SSN [REDACTED]	3. DIVISION [REDACTED]
4. HOME ADDRESS (Street, City, State, Zip Code) [REDACTED]	5. MODE(S) OF TRANSPORTATION TO BE USED DAILY TO COMMUTE TO AND FROM WORK. <input type="checkbox"/> Bus <input type="checkbox"/> Light Rail <input checked="" type="checkbox"/> Subway <input type="checkbox"/> Ferry <input type="checkbox"/> Train <input type="checkbox"/> Authorized Vanpool <input type="checkbox"/> Other (Specify)	6. TYPE OF FARE MEDIA YOU USE. SmarTrip Card (Card No.) [REDACTED] <input type="checkbox"/> Fare card <input type="checkbox"/> Tickets <input type="checkbox"/> Pass <input type="checkbox"/> Tokens <input type="checkbox"/> Voucher <input checked="" type="checkbox"/> SmarTrip Card <input type="checkbox"/> Other (Specify)
7. WORK TELEPHONE NUMBER [REDACTED]	8. MONTHLY COMMUTING COSTS (from worksheet on back) \$142.00	

EMPLOYEE ACKNOWLEDGEMENT AND CERTIFICATION

- I certify I am employed by the Federal Election Commission.
- I certify I am eligible for a public transportation fare benefit. I will use it for my daily commute to and from work. I will not give, sell, or transfer it to anyone else.
- I certify I am not a member of a carpool. Furthermore, I do not receive disability or executive parking privileges.
- I certify that the monthly transit benefit I receive does not exceed my monthly commuting costs.
- I certify that in any given month, I will not use the Government-provided transit benefit in excess of the statutory limit. If my commuting costs per month exceed the monthly statutory limit, I will supplement those additional costs with my own funds.
- I certify I am responsible for returning unused FEC funded fare subsidy to the Office of Finance no later than my effective date of resignation, transfer, retirement, etc. from the FEC.
- I certify my usual monthly public transportation commuting costs (excluding any parking costs) is the amount listed above (amount is supported by completed worksheet).
- I understand that I must submit a new Transit Subsidy Program Participant application if there is any permanent change in the information provided above.
- I understand that it is a Federal crime under 18 United States Code, Section 1001, to make a false fictitious or fraudulent statement on this form. If I make a false statement, I may be subject to criminal prosecution and punishment, including a fine and/or administrative punishment, which may result on

09 FEB 12 PM 12:12

[REDACTED]	12. DATE 2/12/09
------------	---------------------

**APPROVED BY THE HUMAN RESOURCES OFFICE
NAME - HR BENEFIT COORDINATOR**

13. NAME OF HR BENEFIT COORDINATOR	14. AGENCY MAXIMUM BENEFIT (Enter monthly payable amount for each participant based upon commuting costs, statutory limitations, agency policy, Union Negotiations, etc.).
15. SIGNATURE OF HR BENEFIT COORDINATOR	16. DATE
17. ENTERED IN METRO SYSTEM AND FEC DATABASE BY:	18. DATE

PRIVACY ACT STATEMENT

This information is solicited under authority of Public Law 101-509. Furnishing the information on this form is voluntary, but failure to do so may result in disapproval of your request for a public transportation transit fare benefit. The purpose of this information is to facilitate timely processing of your request, to ensure your eligibility, and to prevent misuse of the funds involved. This information will be provided to the Human Resources and Finance to administer this program and to ensure that you are not listed as a carpool participant or a holder of any other form of vehicle work site parking permit with FEC or any other Federal Agency.

CALCULATION OF COMMUTING COST

To be completed by applicant: Use Appropriate Daily and/or Monthly Costs to calculate your costs per month. **Note: Do not include parking costs.**

Mode of Transportation	Daily Costs (round trip)	Multiplied by # of work days (20 for F-T)	Equals Monthly Commute Costs
Subway (METRO)	\$ 7.10	Multiplied by 20 work days	\$ 142.00
Metro Bus	\$	Multiplied by work days	\$
Commuter Train (VRE, MARC, etc.)	\$	Multiplied by work days	\$
Other Bus (e.g., Ride-On)	\$	Multiplied by work days	\$
Van Pool	\$	Multiplied by work days	\$
Other	\$	Multiplied by work days	\$
Total – all costs	\$ 7.10	Multiplied by work days	\$ 142.00

Routing Pattern (Required) [redacted] to Metro Center and return
Metro Center to [redacted] and return

Example 1: Vienna to Metro Center and return

Example 2: Line 1 Bus from residence to New Carrollton
 Line 2 Metro to Navy Archive and return. Bus back to residence.

**FEDERAL ELECTION COMMISSION
TRANSIT SUBSIDY PROGRAM APPLICATION**

(Please type or print legibly in blue or black ink)

ACTION REQUESTED (CHECK ONE): New Change Cancellation Annual Recertification Temporary NTE
DATE:

NOTE: Items 1 through 12, and the reverse side of this form must be completed in full before submitting to Human Resources.

APPLICANT INFORMATION

1. NAME OF APPLICANT (Last, First, Middle Initial) [REDACTED]	2. LAST FOUR DIGITS OF SSN [REDACTED]	3. DIVISION [REDACTED]
4. HOME ADDRESS (Street, City, State, Zip) [REDACTED]	5. MODE (S) OF TRANSPORTATION TO BE USED DAILY TO COMMUTE TO AND FROM WORK. <input type="checkbox"/> Bus <input type="checkbox"/> Light Rail <input checked="" type="checkbox"/> Subway <input type="checkbox"/> Ferry <input type="checkbox"/> Train <input type="checkbox"/> Authorized <input type="checkbox"/> Vanpool <input type="checkbox"/> Other (Specify)	6. TYPE OF FARE MEDIA YOU USE. SmarTrip Card (Card No.) [REDACTED] <input type="checkbox"/> Fare card <input type="checkbox"/> Tickets <input type="checkbox"/> Pass <input type="checkbox"/> Tokens <input type="checkbox"/> Voucher <input checked="" type="checkbox"/> SmarTrip Card <input type="checkbox"/> Other (Specify)
7. WORK TELEPHONE NUMBER [REDACTED]	8. MONTHLY COMMUTING COSTS (from worksheet on back) \$ 142.00	

EMPLOYEE ACKNOWLEDGEMENT AND CERTIFICATION

- I certify I am employed by the Federal Election Commission.
- I certify I am eligible for a public transportation fare benefit. I will use it for my daily commute to and from work. I will not give, sell, or transfer it to anyone else.
- I certify I am not a member of a carpool. Furthermore, I do not receive disability or executive parking privileges.
- I certify that the monthly transit benefit I receive does not exceed my monthly commuting costs.
- I certify that in any given month, I will not use the Government-provided transit benefit in excess of the statutory limit. If my commuting costs per month exceed the monthly statutory limit, I will supplement those additional costs with my own funds.
- I certify I am responsible for returning unused FEC funded fare subsidy to the Office of Finance no later than my effective date of resignation, transfer, retirement, etc. from the FEC.
- I certify my usual monthly public transportation commuting costs (excluding any parking costs) is the amount listed above (amount is supported by completed worksheet).
- I understand that I must submit a new Transit Subsidy Program Participant application if there is any permanent change in the information provided above.
- I understand that it is a Federal crime under 18 United States Code, Section 1001, to make a false fictitious or fraudulent statement on this form. If I make a false statement, I may be subject to criminal prosecution and punishment, including a fine and/or administrative punishment, which may result on the termination of my federal employment.

12. DATE
7/9/09

APPROVED BY THE HUMAN RESOURCES OFFICE
[REDACTED] - HR BENEFIT COORDINATOR

13. NAME OF HR BENEFIT COORDINATOR [REDACTED]	14. AGENCY MAXIMUM BENEFIT (Enter monthly payable amount for each participant based upon commuting costs, statutory limitations, agency policy, Union Negotiations, etc.)
15. SIGNATURE OF HR BENEFIT COORDINATOR [REDACTED]	16. DATE 7/14/09
17. ENTERED IN METRO SYSTEM AND FEC DATABASE BY: [REDACTED]	18. DATE 7/10/09

PRIVACY ACT STATEMENT

This information is solicited under authority of Public Law 101-509. Furnishing the information on this form is voluntary, but failure to do so may result in disapproval of your request for a public transportation transit fare benefit. The purpose of this information is to facilitate timely processing of your request, to ensure your eligibility, and to prevent misuse of the funds involved. This information will be provided to the Human Resources and Finance to administer this program and to ensure that you are not listed as a carpool participant or a holder of any other form of vehicle work site parking permit with FEC or any other Federal Agency.

CALCULATION OF COMMUTING COST

To be completed by applicant: Use Appropriate Daily and/or Monthly Costs to calculate your costs per month. Note: Do not include parking costs.

Mode of Transportation	Daily Costs (round trip)	Multiplied by # of work days (20 for F-T)	Equals Monthly Commute Costs
Subway (METRO)	\$ 7.10	Multiplied by 20 work days	\$ 142.00
Metro Bus	\$	Multiplied by work days	\$
Commuter Train (VRE, MARC, etc.)	\$	Multiplied by work days	\$
Other Bus (e.g., Ride-On)	\$	Multiplied by work days	\$
Van Pool	\$	Multiplied by work days	\$
Other	\$	Multiplied by work days	\$
Total - all costs	\$ 7.10	Multiplied by 20 work days	\$ 142.00

Routing Pattern (Required) [redacted] to Metro Center and return
 Metro Center to [redacted] and return

Example 1: Vienna to Metro Center and return

Example 2: Line 1 Bus from residence to New Carrollton
 Line 2 Metro to Navy Archive and return. Bus back to residence.

Employee Enrollment Modification Process

CUSTOMER ID: [REDACTED]

SmarTrip Card Number:	[REDACTED]
First Name:	[REDACTED]
Middle Initial:	[REDACTED]
Last Name:	[REDACTED]
Status:	<input checked="" type="radio"/> Enrolled <input type="radio"/> Removed
Kickoff Date:	09/01/2007 (mm/dd/yyyy)
Benefit Category Type:	142 - \$142 PER MONTH
User Defined Key:	[REDACTED]

[Save](#) | [Reset](#) | [Close](#)

Click this [Suspend/Restore Benefits](#) button to suspend/restore the benefits.

!!! Employee has been updated successful !!!

Attachment No. 4

Email from [REDACTED]
to [REDACTED]
dated 09/23/08

Case Number INV-09-01

[REDACTED]
05/03/2010 05:52 PM

To [REDACTED]
cc
bcc
Subject Fw: Transit benefit program

----- Forwarded by [REDACTED] FEC/US on 09/23/2008 12:36 PM -----

[REDACTED]
09/23/2008 11:24 AM

To [REDACTED]
cc [REDACTED]
Subject Transit benefit program

Good morning [REDACTED]

We are updating our records as part of an overall review of the employee transit benefit program and would appreciate your assistance in this effort.

Based upon information I have received for the period April 1, 2008 to October 1, 2008, you have claimed \$115 in transit benefits for the past six months. However, it appears that you are also parking in the FEC garage which is not permitted under the employee transit benefit program. If you are currently parking in the garage, your participation in the transit benefit program will be suspended, however, you may re-enroll in the transit subsidy program, by contacting the Human Resources Office, when commuting to the FEC using public transportation.

Please contact me by Monday, September 29, if the information I have is inaccurate or outdated otherwise I will remove your name from the transit benefit program effective October 1, 2008. Again, you are eligible to re-enroll in the transit benefit program when you commute to the FEC using public transportation. In order to determine if it is necessary to reimburse the Agency for transit benefits that were claimed while simultaneously parking in the garage, please let me know when you began to park in the garage and we will review it.

Please feel free to contact me and again, thank you for your assistance.

[REDACTED]

[REDACTED]
Office of Human Resources
U.S. Federal Election Commission
999 E Street, NW
Washington, DC 20463
(Tel) 202-694-1085

Attachment No. 5

Kastle Systems History Reports
for keycards assigned to



Case Number INV-09-01

Attachment No. 6

FEC Temporary Parking Permit Sign-out Sheets
obtained from
the Administrative Services Division.

Case Number INV-09-01

February 23, 2009



[Redacted]

Office of Inspector General
999 E. Street, NW, Suite 940
Washington, DC 20463

Re: PARP Request No. 08-0381

[Redacted]

Dear [Redacted]:

This is regarding the request that was submitted by [Redacted] Federal Election Commission on November 13, 2008. The request was for copies of SmarTrip transactions for card [Redacted] for September 1, 2007 - present. Specifically, [Redacted] requested the dates and amount of SmarTrip benefit draws and details of usage activity, to include dates, times, and metro stop locations where benefits were used. The request was made in connection with an on-going investigation. The request was processed pursuant to Metro's Public Access to Records Policy (PARP) and Privacy Policy. Both policies can be viewed on our website at http://www.wmata.com/about_metro/public_rr.cfm, under the section marked, "Legal Affairs." On December 12, 2008, we provided the records. Then on February 5, 2009, you notified us that we did not include the exit and entry times.

Enclosed are the transactions which include the exit and entry times. For your information, although our records reflect that SmarTrip card [Redacted] is registered to [Redacted], we cannot verify that [Redacted] is the individual who used the card. Generally, SmarTrip records are not available to anyone other than the registered owner. However, these records are being released to you in accordance with PARP section 6.1.8(b) and Privacy section 6.1(d), which provide for release to law enforcement officials who meet the requirements of these sections.

There is no charge for the enclosed records because the first two hours of staff time and minor copying are free. Future correspondence regarding your request should be directed to my attention and should reference the PARP request number above. You may also contact me at 202-[Redacted].

Sincerely,
[Redacted]

PARP/Privacy Policy Administrator

Enclosure

**Washington
Metropolitan Area
Transit Authority**

400 Fifth Street, NW
Washington, DC 20001
202/962-1234

By Metrorail:
Ferry Square—Red Line
Navy Yard—Blue Line
Union Station—Red, Green and
Yellow Lines
By Metrobus:
Routes D1, D3, D6, P6,
70, 71, 80, X2

Attachment No. 9

Clifton Gunderson Report on FEC Data Concern

Case Number INV-09-02

FEDERAL ELECTION COMMISSION

REPORT ON DATA CONCERN

June 2, 2009

This report includes proprietary and confidential data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this report. This restriction does not limit the Government’s right to use information contained in this report if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets marked with the legend “Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this report.”

Report on Federal Election Commission Data Concern

Overview

On February 11, 2009, Clifton Gunderson (CG) initiated an internally led investigation regarding the evaluation of the controls and circumstances surrounding a potential security concern of Federal Election Commission (FEC) data. The incident in question is related to CG having provided/loaned a CG owned laptop to the Federal Communications Commission (FCC) Office of Inspector General (OIG). CG provided this laptop to the FCC OIG for the purpose of allowing them to review working papers related to the FCC annual audit. However, this laptop contained data which CG should have deleted from the machine related to the FEC 2007 audit. Therefore, there was FEC data which CG inadvertently disclosed to the FCC OIG representatives. Some of this data was sensitive IT system data, containing machine names and IP addresses related to the FEC's IT network, which could pose a security risk to the FEC. Based on CG's understanding, this data was not disclosed outside of the FCC OIG.

It was determined that an information technology (IT) auditor ("Auditor"), outside and independent of the CG Federal IT group and practice, would be appointed to conduct the procedures related to this incident. CG's MACSC Commercial IT Assurance Leader ("Auditor") was selected to execute procedures regarding the circumstances of this incident.

The Auditor received a list of questions and concerns from the FEC OIG office on February 13, 2009. Based primarily on these questions which the FEC requested be addressed, the Auditor developed an audit program. This program consists of policy and procedure inquiries and observations, specific interview topics and interviewees, and additional test procedures. The items in the audit program were cross-referenced to the FEC OIG question list to determine coverage of the items raised by the FEC.

The procedures performed for this investigation were conducted over the period of February 18, 2009 to April 6, 2009. This report outlines a summary of the questions raised by the FEC, the procedures performed relative to those questions, and a list of observations and recommendations identified by the Auditor.

Clifton Gunderson LLP

Calverton, Maryland
June 2, 2009

Questions and Procedures:

- The FEC OIG requested that a description and timeline of the laptop and incident in question be prepared.
 - CG performed interviews and obtained specific evidence (including sign-out sheets, fixed asset database listings, and inventory reconciliations) to validate a timeline and to document the chain of custody with the laptop in question. The interviews were with internal CG personnel, and included the:
 - IT Audit Senior Associate
 - IT Audit Manager
 - Services Operations division, including Manager and Director
 - IT Engagement Partner for FEC and FCC engagements
 - FEC Engagement Partner; and,
 - Calverton Office Partner in Charge (PIC) and Federal Practice Lead Partner
- The subcontractor assigned the laptop was also interviewed, as well as the owner of the consulting company the subcontractor is employed at. Further details and outlines of the interviews conducted and responses are illustrated in Appendix B: “Summary of Interviews Conducted”.
- Observation noted regarding tracking and accuracy of laptop sign-out sheets and tracking (See Observation #1).
-
- An accounting of laptops used by CG and subcontractors and delete FEC data from identified laptops.
 - CG obtained and reviewed listings of employees who charged time to the FEC engagement, reviewed FEC OIG listing of employees and laptops identified with property passes, and reconciled laptops used and traced to current location/employee. CG also swiped all loaner machines and unassigned machines.
 - Observation noted related to tracking of computer disposal (See Observation #2).
 - CG attempted to review all employees back to 2004. However, due to the fact that the current process and tracking database for fixed assets was only implemented in late 2006; there is a limitation in the ability to reconcile all employees and laptops as tracking in 2004-2006 is limited or non-existent. All asset tag numbers identified in the FEC property pass listing were able to be reconciled, and the history of any re-assignment of the laptops internally at CG was also noted. One serial number had a transposition error in the property pass log, but was still reconciled. Further, there were a total of 4 machines that could not specifically be located within CG. These laptops were machines that belong to subcontractors or provided to the FEC. Two of these machines were for subcontractors whom were only used in 2004 (when all subcontractors used their own laptops), and another was assigned to the subcontractor used to do IT work in 2007. It was validated through interviews with CG managers, partners, Service Operations, and the subcontractor, and via understanding with FEC contacts as well, that this individual logged both the laptop provided to him by his firm, as well as the CG machine. This is confirmed via the reconciliation and testing of the property pass information from the FEC. Further, the last machine which could

not be located was a machine assigned to the FEC CG Audit Manager, who had provided it to the FEC OIG for purposes of w/p review. The Auditor confirmed with the FEC OIG contact that this machine was in their possession.

- Description of the synchronization and upload process of engagement data to the CG server and procedures relative to removal of data.
 - CG obtained and reviewed the end user standards policy, the Risk Management manual, and the IT Manual. Determined that these policies and procedures include provisions relative to KillDisk swiping, requirements for removal of data from local files, and confidentiality/non-disclosure of client data. The mechanism for the update and synchronization was reviewed with the [REDACTED] office [REDACTED] Engagement “Champion”, who is responsible for trainings relative to that software, and with Service Operations. The procedures for synchronization at CG through [REDACTED] are based on files (engagements) for clients being maintained at a [REDACTED]. The [REDACTED] is maintained in [REDACTED]; and is accessed by other offices and regions of CG through [REDACTED] access. [REDACTED] allows for the synchronization of data from the [REDACTED] to one of two locations. Staff can synchronize data to their desktop directly; or they can synchronize the engagement to their [REDACTED] “Local File Room”. Access to the CG network is required to perform synchronization. Binder packages can also be created from within [REDACTED] which will create local copies of files. This functionality is utilized and needed in situations whereby the audit teams do not receive internet/network access at the clients they are working at. Further, there is peer-to-peer synchronization capability, for users to connect machines directly to copy/synch data. Data may also be copied via binder packages sent through email or via USB drive or CD, but would need to be loaded into [REDACTED] to be accessible.
 - Some of the specific details outlined in the documentation reviewed includes:
 - Risk Management Manual. CG’s Risk Management Manual is 27 pages, and is posted on the CG Intranet (CGConnect). It includes sections related to “Records Retention” requiring only one year of prior client data be accessible through [REDACTED] Engagement. It has a section on “File Location and Maintenance” which prohibits personal copies of any client information or data; requiring all data to be stored in the central file room and/or the client engagement files. This Manual also articulates rules relative to “Client Information on Laptop Computers.” This section lists seven rules to follow regarding use of laptops; including not to leave laptops unattended, using cable locks to secure computers, not leaving laptops in vehicles, not sharing of passwords with anyone, and backing up of client data.
 - IT Manual. CG’s IT Manual is 18 pages, and is available via the intranet. It includes sections on CG’s encryption policy which requires [REDACTED] minimum encryption be loaded on all laptops. Further, it includes sections on “Acceptable Use Policy” and lists specific unacceptable practices such as any installation of non-firm approved and sponsored software, unauthorized copying or transmission of client data, use of streaming media, revealing password or account information, or use of CG laptops for any activity in violation of CG harassment policies or EEO policies. The policy also includes sections to outline guidelines and requirements for “Email and

- Communication” activities. Lastly, it includes sections and specific workflow documentation for the process and procedures relative to computer disposal. This workflow includes 2 options for computer disposal; for low risk items where the machine is being reused, Format and Reimaging of the drive occurs. For machines being disposed of (no longer owned/assigned by CG) then a utility called KillDisk is run to wipe the drive.
- Service Operations, the internal IT technical support group within CG, also maintains internal procedures related to executing the KillDisk procedures. These were reviewed as part of the Auditor’s procedures. They include specific screen shots and instructions and are titled “Steps for disposal of Desktop/Laptop.” The instructions specifically list (in step 3D) to use “erase Method: US DOD 5220.22-M (slow, High Security).”
 - No observations.
- Policies and procedures regarding disposal of laptops.
- CG reviewed the procedures regarding disposal of laptops, including procedures relative to Workstation Setup/Configuration and KillDisk procedures. In addition to the IT Manual and procedures listed above; CG Service Operations also maintains a “Workstation Setup Checklist.” For transfer of laptops; the workstation setup checklist would be what applies (during format and reimaging). The procedures within this checklist include the reimaging of the drive; deletion of the machine from SMS and Active Directory; reloading profiles; installation of audit software needed; deleting [REDACTED] recovery files assigned to previous profiles; mapping [REDACTED] drives; etc.
 - Observation noted regarding documentation of disposal (See observation #2).
- Information regarding prior incidents or data/security breaches.
- CG inquired of the Director of Service Operations regarding tracking of incidents. There is no formalized or centralized process firm-wide at CG for tracking of incidents or security issues. This is handled informally at the Client Service Center (CSC) level. The Auditor coordinated with the Director of Service Operations for the Mid-Atlantic region to coordinate with corporate IT, as well as other Service Operations Managers in other CSC locations. As of April 11, 2009, the Auditor received information detailing a number of incidents. The incidents occurred in the [REDACTED] offices. The [REDACTED] incident is the most recent, and is the incident which is the basis for this report and investigation. This incident is related to the assignment of a machine to a federal agency (FCC) for purposes of w/p review, with mistaken data still on the machine. In addition to this incident, there are eight other incidents noted/reported. These other eight all relate to stolen laptops or data. Six of the incidents relate to stolen laptops, and another relates to stolen work papers. These incidents occurred in 2007 and 2008. In one of the incidents related to a stolen laptop from the Arlington office, the computer was recovered by the police and returned to CG. Further, the Auditor reviewed the users noted as being responsible for, and assigned to, the laptops involved in the [REDACTED] incidents. The Auditor compared this list to the users who charged time to the FEC engagement since 2004. With the exception of the incident being reported on in this investigation,

none of the other laptops listed were in use by, or assigned to, any employee who worked on the FEC engagement.

- No observations.

○ Determine password policies and procedures.

- CG reviewed desktop account and password controls and setting for reasonableness, and CG communication and acceptable use policies. CG has a separate Communications Policy, which employees receive and acknowledge. This policy outlines requirements for internet communications, restrictions of access to systems, unauthorized access, and that electronic communications with CG equipment is CG's property, and that laptops are for business use only.

- The Password and Account features required at CG include:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- Observation noted See Observation #7 regarding [REDACTED] password requirements.

○ Evaluate the circumstances of the password and username written on the laptop.

- CG performed interviews to determine the circumstances and timing/accountability for writing the password for the network and [REDACTED] engagement ID and password. The account and password to the [REDACTED] application were written down, as was the userID for the laptop (Windows). However, the password to Windows was written down per the request of the FCC OIG representative. This point was covered during the interview with the IT Audit Senior Associate, and was also discussed briefly with the FEC OIG investigator, who did have access to interview the FCC OIG representative. The FCC OIG contact indicated that "may have been" the circumstances but that he didn't really recall what had transpired. The CG Senior Associate believes this is how it happened, but wasn't sure whether there was specific request to write down the

Windows password, or the precise circumstances but that she knew it was written down in front of the FCC OIG contact, and that she believed he requested that she write this down for him.

- Observation Noted See Observation #3.
- Describe physical security controls and procedures, as well as security procedures and training to employees.
 - CG reviewed the IT Manual, the Risk Management manual, the Communications policy, and End User Requirements as published at CG. Additionally, the controls regarding the physical security (keys/fobs, etc.) for the secure storage areas at the CG office locations were observed and evaluated. Administrative staff, office Partners-in-Charge (PICs), and Service Operations staff all maintain keys or fobs (or both) for the secure storage areas within CG offices ([REDACTED] specifically observed). Lastly, regarding security training or notice, the SecureIT notices and communications to CG employees were reviewed. The IT Manual, Communications Policy, and End User Policies are all communicated to employees upon being hired. The IT Manual and End User Policies are available via intranet as well. SecureIT messages, via email and office communications (including postings in break rooms) are used to communicate “hot topic” updates on security and related topics.
 - Observation Noted See Observation #4.
- Review the encryption process and utilities used for CG laptops.
 - Auditor observed encryption tools, reviewed the encryption authentication process, and performed interviews to determine timing of implementing encryption onto laptops. The asset tracking database also was reviewed to determine the loading/implementation of the [REDACTED] encryption tool. The encryption utility is [REDACTED]. [REDACTED] is a required loadset (per the CG policy and Manuals listed above), and was installed on all machines during the middle of 2007. The authentication method for [REDACTED] is a “pass through” authentication of the Windows logon (ID and password). This essentially states that a separate logon and authentication process for [REDACTED] does not exist; therefore, two-factor authentication is not used, since the same account and password for Windows is used to authentication [REDACTED], as well. A communication was sent to the FEC CIO regarding this distinction in CG authentication requirements in September 2007 regarding this exception.
 - Observation Noted See Observation #8.
- Prepare a timeline of the laptop incident.
 - CG has developed a timeline in Appendix A of this report.
- Determine CG’s incident response policies.
 - Auditor reviewed SecureIT communications and notices distributed to CG employees. Also reviewed the incident response procedures and reporting template. The incident response process is outlined in sections within the IT Manual regarding items and situations which require notification and communication to the Help Desk and/or Service Operations. The tracking information and templates have instructions and indicate where the data and information needs to be saved on the network and

where submitted to. The information collected and monitored via the incident tracking form includes:

- Who reported the incident
 - Contact information
 - Incident Date, Time, and current status of the incident
 - Type of Incident and description; as well as perceived impact
 - Systems affected
 - Loss of Data incurred and Actions Taken
 - Resolution suggested
 - Data/Time when Incident was/is closed
 - Team Members assigned to review/address the incident
 - Manager sign-off.
 - No observations.
- Determine CG's system policy regarding administrators and multiple user accounts.
- CG reviewed the system capabilities and determined that multiple user accounts or profiles can be created on the same laptop. Due to the fact loaner machines, as well as individual laptops, may be used by multiple staff; the presence of multiple accounts/profiles on laptops is not deemed to be an exception. Further, based on the process outlined above regarding synchronization of data since any staff can access an engagement via the Central File Room (at least related to synchronized the past year files/data for clients), the risk of multiple profiles or accounts appears minimal. As it relates to administrators, there are administrator profiles loaded, as these are used by the Service Operations to assist with computer, application, and etc. issues. Also, these accounts exist since those staff reimage and format the drives.
 - No observations.
- Explain CG laptop inventory processes and laptop pool concept, as well as assignment of computers to subcontractors.
- CG determined that an inventory process occurs, through review of inventory tracking sheets (physical inventory tracking), fixed asset tracking database, and performed interviews to understand processes relative to loaner pools for laptops. Also, reviewed the procedures for providing laptops to subcontractors. The fixed asset tracking database is used to track the location and history of machines. This is a Microsoft Access database which is administered and maintained by Service Operations. There is also a separate Microsoft Excel spreadsheet used to keep as a "backup" to the tracking database. Also, once or twice a year (per interview with Service Operations and observation of inventory tracking spreadsheet) a physical inventory and tracking of devices is performed. Microsoft's SMS tool is also used by Service Operations in order to identify and track the laptops used to login to the CG network. CG procedures regarding providing loaner laptops to clients or subcontractors involves completing the Workstation Setup Checklist and procedures illustrated previously, and to then have the tracking database updated, and the laptop user history revised accordingly within the database and tracking spreadsheet backup.
 - Observation Noted See Observations #1 and 2.
- Determine CG's IT awareness processes, training, and documentation.

- CG determined that SecureIT communications are used for communication of security awareness concerns and topics; that email communications are sent to employees for security notices, and that laptop security controls are included with End User Requirements and IT Manuals which are available and provided to CG employees. Also, verified that those employees on the FEC engagement attend specific security awareness training. This was determined through review of a signed acknowledgement document which also accompanies a signed non-disclosure document with the FEC. All employees who charged time in 2007, per the CG time tracking system report obtained by the Auditor were noted as having participated in the FEC required Security Awareness training (via signed acknowledgements) as well as the subcontractors. Additionally, these individuals also signed agreements regarding Non-Disclosure of FEC data. These forms were obtained and reviewed by the Auditor, as well. Lastly, as described previously, CG's Communication Policy which employees receive also includes specific requirements relative to security and unauthorized use of CG systems and laptops.
 - No observations.
- Provide information on the practices of permanently deleting (wiping) of CG laptops.
 - Auditor performed interviews and review of KillDisk procedure documentation and IT Manual to determine the processes and procedures for deleting client data and wiping of data. Details of KillDisk procedures and related IT Manual sections are articulated above.
 - Observation Noted See Observatin #2.
 - Update Effective 2/27/2009, Service Operations will run KillDisk on all transferred or returned loaner machines. Prior, CG only ran KillDisk for disposal of laptops, and reformatted drives only during transfer of laptop to another employee (not necessarily if kept in loaner pool).
- Provide CG policies and procedures on protection of PII.
 - Auditor performed interviews and review of CG Risk Manual, procedures, policies, IT Manual, and Audit Manual. Also reviewed CG template forms and terms/conditions. Determined that various policies and procedures exist relative to controls and procedures regarding client data. While PII is not specifically indicated, the procedures previously noted (such as IT Manual, Risk Management Manual, End User Procedures, Communications Policy, etc.) apply to all client data, and illustrate that client data in general is to be treated as confidential. Further determined that policies are in place regarding non-disclosure of client data.
 - No observations.
- Identify security logs utilized on CG laptops.
 - Auditor performed interviews and reviewed desktops, including account policies and settings under the windows configurations, including Event Viewer and audit policy. The audit policy is set to log account logon successes, audit logon event successes, and successful and failed system events. Also, within [REDACTED], for engagements that are "In Process" status, a log of [REDACTED] synchronizations is maintained. Once an engagement is finalized, this history is no longer available. This was determined via

observation, as well as through inquiry with CG IT and Service Operations. Per observation of the Auditor's CG laptop, the Event Viewer configuration is to "Overwrite Events As Needed", with the log size set to 40960 KB for the Application and System logs, and 131072 KB for the Security log size.

- No observations.
- Inquire whether subcontractors, or staff, use personal laptops for CG business.
 - CG performed interviews, did observation, and obtained representations regarding use of other laptops. Determined that personal computers are not used, but that subcontractors do/may use their own company supplied laptops for use on CG engagements. Received representation from subcontractor related to this incident, and his firm, that FEC data had been deleted from laptop(s) used during subcontracting arrangement.
 - No observations.
- Inquire why the FEC data was not deleted from the laptop which was provided to the FCC OIG.
 - Through the interviews performed (see Appendix B), documentation reviewed [including laptop inventory logs, loaner machine sign-in/sign-out sheets, workstation configuration checklists, and others], and review of the laptop image and files; there appear to be a number of contributing factors regarding the data not being removed. These factors include:
 - CG procedures when finalizing engagement files through [REDACTED] software indicate that the engagement partner will finalize his/her review, and then notify all team members to remove/delete all related data from their local file room, or local copies of [REDACTED] binders. However, since this machine had been returned from a subcontractor at the time the binder was finalized; it appears to have been overlooked in the process to delete the data upon engagement finalization.
 - Procedures also indicate that upon machines transferred between employees or from subcontractors, that the laptop should be reimaged (thereby deleting the data). In this case, the sign-in/sign-out controls were not enforced and the procedures to log machines being removed from or returned to the loaner pools were not followed. This led to the fact that a workstation configuration checklist form was not completed, and Service Operations did not reimage the drive, as would be indicated by CG procedures.
 - The [REDACTED] directory structures within Windows Explorer were renamed. [REDACTED], as most standard software programs, has a file/directory structure it utilizes to operate, to store executables, to store files, etc. Apparently, in March 2008, [REDACTED] was reinstalled on the laptop. At that time, it seems that the prior [REDACTED] directory(ies) were renamed to "[REDACTED] Engagement.old". The ".old" portion is not standard naming convention, and would likely have been done in order to preserve prior [REDACTED] data during the reinstall. This directory was never later removed or deleted. This created additional factors, as during the transfer of this laptop to the FCC OIG, Service Operations did instruct the IT Senior on how to remove all [REDACTED] data, which was performed. However, again, since the data was now in a renamed folder/directory, the process to remove [REDACTED] data

was not successful, as it removed data from the [REDACTED] Engagement” directory, and not the folder which had been renamed to “.old”.

Summary of Observations:

1. While a tracking spreadsheet and sign-in/sign-out log is maintained for machines, when the laptop was returned by the subcontractor, the machine was not registered on the sign-in/sign-out log when it was returned in the autumn of 2007, and does not appear to have been updated/notified to Service Operations. Additionally, it appears that there were other times at which this machine was used for various reasons in 2008, and the machine was not logged in or out on the tracking sheet, or the sign-out log in Calverton. CG procedures are to reformat computers when transferred, but this was not done in this case as a result of the breakdown in tracking.
 - a. RECOMMENDATION: Only Service Operations should be involved in tracking and updating computer/laptop assets. The process for tracking laptops and devices should be centralized, rather than separate office and Service Operations procedures and processes.
 - i. UPDATE As of 2/27/2009; the Director of Service Operations, required that all machines being transferred or used within the laptop pool are required to have KillDisk run against them to swipe the drives, instead of reformatting the drives.
2. Evidence of computer disposals and running of KillDisk utility is not retained.
 - a. RECOMMENDATION: CG should ensure that the fixed asset log maintains a history of all machines. This history should include details of when machines are disposed, evidence of reviewing/confirming that KillDisk is run on the machine, and where it is sent upon disposal (i.e. charity, internal, client, etc.).
3. Post-It Note with Account and Password data taped to laptop. It is likely and reasonable that FCC OIG requested that the windows account password be also written on the laptop; but policy should dictate that CG personnel not write down passwords in any situation.
 - a. RECOMMENDATION: Do not include any account and password data when provided loaned laptops. Only provide this information verbally. If client requests this data to be written, CG should indicate that that request to do so must be submitted to and approved by the engagement partner before any data of that nature is provided in written format.
4. Perhaps as a result of a contentious email from the FCC OIG, partners made determinations to proceed and use a “pool” laptop in order to expedite the OIG request for a new machine to review working papers. The laptop was not directly reviewed by Service Operations and wasn’t reformatted before providing to the FCC; although Service Operations was consulted via phone in setting up the machine. Further, physical security restrictions to loaner pools is not adequately restricted and monitored.
 - a. RECOMMENDATION: Only Service Operations should be allowed to provide laptops/devices to clients/subcontractors. Since they maintain the procedures and checklists for preparing laptops, they should be required to be involved in these situations directly; unless specifically approved (in writing) from a partner.
 - b. RECOMMENDATION: Additionally, it is suggested that only Service Operations and PICs have access to the computer storage areas in each office. This should help to more closely control and monitor the computer and device assets.

5. While contracts exist with SamLin consulting; there is nothing specific articulated in those contracts relative to the FEC engagement. Also, while the subcontractor signed an NDA with the FEC which states not to disclose FEC data; this did not include a section on acceptable usage or other components - such as not using private machine, acknowledging abiding by CG policies on returning/removing client data, not copying data,, not using machines for non-business purposes, awareness of PII/sensitive data, etc. Further, there are currently no procedures or contract provisions to verify that client data is deleted and wiped from subcontractor laptops/desktops.
 - a. RECOMMENDATION: Need to ensure that contracts are updated to include all engagements and task orders leveraging subcontractors, and that these contracts include confidentiality provisions, appropriate usage requirements, indemnification clauses as appropriate, and provisions to abide by CG procedures relative to client data retention and security.
 - b. RECOMMENDATION: Subcontractor contracts and CG policy should be updated to include provisions for CG to verify/validate that client data is deleted/removed from subcontractor laptops timely.

6. Standard contract language does not include provisions for the use of CG laptops or devices. Review of the FCC contract does not have any provisions or requirements for return of equipment, acceptable use of loaned laptops (including restrictions on email policy, internet, etc.), or non-disclosure agreements of data.
 - a. RECOMMENDATION: CG should incorporate contract language or usage agreements with clients or agencies that intend to utilize CG owned equipment and laptops. This language should include agreements regarding acceptable usage of the device, specific timetables, protocols for help desk, and non-disclosure components.

7. ■ Engagement does not have password complexity requirements.
 - a. RECOMMENDATION: CG should consider implementing specific password syntax, intruder lockout, and other requirements to enhance work paper and client data security.

8. Per a letter and communication with the FEC CIO, there was an agreement to remove all FEC data within 90 days from all laptops. This letter was intended to be a waiver on the dual factor authentication provision on CG laptops.
 - a. RECOMMENDATION: Need to monitor such commitments and agreements with clients to validate and ensure conformity with such provisions and expectations.

9. “■ Engagement.Old” directory was renamed in March 2008. This was likely done as a precaution when reinstalling ■ Engagement.
 - a. RECOMMENDATION: CG should update it’s IT Manual and its laptop procedures to include provisions to delete any prior ■ engagement directories. If the practice of renaming the directory is needed as a precaution to protect against data loss; then procedures should dictate that subsequent to confirming a successful reinstall and access to data and ■, renamed and prior directories should be removed.

Appendix A: Timeline Summary

- March 7, 2005. This is the date the laptop in question was purchased by CG.
- April 9, 2007. The first evidence of profiles being created on the machine. This correlates to the timing by which Service Operations likely reformatted the hard drive, which would have removed prior data and profiles loaded.
- April 19, 2007. Service Operations prepared a workstation checklist. This included loading a profile and █████ engagement for the use of a subcontractor at SamLin Consulting.
- June 2007. It appears that this was the approximate time of which CG delivered the machine to the subcontractor to use on the Federal Election Commission (FEC) engagement.
- Other profiles including HR and an administrative person no longer with CG (GRUS8035) are also found on the machine, with creation dates of in 2007.
- In early October 2007, the laptop is returned to CG and is presumably returned to the DC Computer Storage room.
- In March 2008 an additional profile is created. Based on the files found on the laptop image, it appears the purpose of this is to utilize the laptop to conduct on internal FedGov audit training seminar.
- March 12, 2008 on this date, it appears that for some reason, █████ Engagement was reinstalled (as this shows as the create date for the █████ Engagement directory). This is also the date that it appears the prior █████ directory was renamed to █████ Engagement.Old.
- In September of 2008, a laptop (NOT the one in question) is provided to the FCC OIG.
- January 28, 2009. A seemingly harsh email is sent from at FCC OIG to CG. This letter is strong in its tone which apparently heightens tensions with the FCC and CG.
- February 2, 2009. FCC OIG calls to indicate that APG is not working on the laptop provided in Sept. 2008. It is later determined by Service Operations, that APG was not loaded on the machine.
- February 2, 2009. The engagement partner and IT partner meet to discuss the situation. The determination is made at that time to provide the FCC OIG with a replacement machine, rather than taking the time to pick up the laptop and have Service Operations fix/repair it. They instruct an IT senior auditor to pull a loaner machine from the secure storage room, and call Service Operations to go through setting up the machine to deliver to the FCC OIG. The senior signs out the machine on 2/2.
- February 3, 2009. A call takes place between the senior and Service Operations. A new profile (0026Temp) is loaded on the machine... as the profile for the subcontractor had expired, as he had not logged in for more than 90 days. Service Operations also talks to the senior about how to delete all data within █████ and load a new █████ binder package onto the laptop containing the FCC file.
- February 3, 2009. The laptop in question is delivered to the FCC OIG. The senior has already placed a post-it note taped to the laptop listing the █████ userID and password and the windows account (0026Temp). During the meeting when she delivers the machine, there is a collective decision (it is not clearly recalled by either whether the FCC OIG asked for this to be done specifically but both agree it was written down with both of them in acknowledgement and present) to also write down the windows password onto the laptop as well.

- February 9, 2009 Service Operations repairs the original laptop provided to the FCC and reinstalls APG.
- February 10, 2009. FCC OIG reports that FEC data is found on the laptop, and that this represents a potential security breach. On this same day, the IT partner and senior meet with FCC and FEC to discuss the situation, and they also then deliver the original repaired laptop to the FCC.
- On February 11, 2009 Auditor is informed of the situation and between 2/11 and 2/12, he is informed of the situation and specific details and begins to prepare to conduct an audit/investigation into the events and circumstances.
- March 14, 2009. Service Operations and the Auditor observe an image of the laptop in question. Some profiles and last modified dates have been modified during the time the laptop is in possession of the FCC OIG.
- March 31, 2009. Service Operations and Auditor visit the FCC OIG office to view the actual laptop. Attempts to access last login history and event viewer logs are unsuccessful due to configuration to overwrite histories after 7 days.

Appendix B: Summary of Interviews Conducted

The Auditor conducted interviews with the subcontractor, the owner of the subcontracting firm, and various internal CG personnel related to the incident in question; including:

- IT Audit Senior Associate
- IT Audit Manager
- Services Operations division, including Manager and Director
- IT Engagement Partner for FEC and FCC engagements
- FEC Engagement Partner; and,
- Calverton Office Partner in Charge (PIC) and Federal Practice Lead Partner

This Appendix B summarizes the topics and information obtained during the interviews conducted by the Auditor during the investigation. The topics covered are listed, with the responses/discussion that followed outlined in bold.

Interview with IT Senior Auditor (occurred on Feb. 13):

Her role was related to the FCC engagement. She indicated that she had not been involved with any FEC data or the FEC audit engagement.

- Describe the nature of the circumstances and your understanding of the events and circumstances around this matter. Please elaborate on the timing to the extent possible regarding the events in question. Also, please describe the “chain of custody” of the laptop at the time it was provided by technical support until when it was delivered to the client.

Reviewed the following timetable and events:

- **In September of 2008, an initial laptop was provided to the FCC OIG for the purposes of reviewing IT w/p’s in █████ software, associated with the FCC financial audit engagement.**
- **She had not had any contact with FCC regarding issues with the computer until February 2, 2009.**
- **Feb. 2: She was contacted by the FCC regarding APG not working, although she had not heard anything between September and February regarding the computer.**
 - **Feb. 2 – She contacted the FCC Engagement Partner and the IT Partner for FCC, regarding the issue with the FCC laptop.**
 - **She contacted the technical support group, Service Operations. They discussed having the computer returned to technical support to fix the issue. She asked if she could load an APG onto a USB drive to deliver a fix sooner. Service Operations indicated to her that this wasn’t within company policy due to licensing issues. She then followed up with the IT and Engagement Partners.**
 - **In order to do something quickly, the decision was made by those partners to switch out the laptop with a “loaner” machine that may be available.**

- She then coordinated with an administrative person in the Calverton office to pull a “temp” laptop out of the locked storage area in the [REDACTED] office, as she did not have access to this area.
 - The laptop pulled was labeled with “[REDACTED]” on it. It wasn’t until later, she was able to determine that [REDACTED] may be a reference to the subcontractor who had worked on the FEC engagement in 2007.
 - She then signed out the laptop from the storage room.
 - She then coordinated with Service Operations over the phone to determine a profile to create on the machine, load APG and the [REDACTED] binder package. She then also coordinated over the phone to delete items in the “Recycle Bin” and also to delete all other [REDACTED] binders through [REDACTED] Engagement. The profile loaded was “0026Temp.”
 - Feb. 3: New laptop was delivered to FCC OIG and she picked up the other laptop to fix APG.
 - Feb. 6: FCC OIG called to indicate he was “looking around” and he found FEC related data and files. He indicated to her that the data wasn’t within [REDACTED], but that he found it in reviewing other directories. She asked him how/where he found it, but he told her “that is not the point. The point is that the data is on there..” and did not elaborate as to how he came across the data. He also informed her at this time that he did not want his other FCC loaned laptop to be shared or sent to anyone else.
 - She worked with the IT partner asap on this report, and they called the FCC OIG back together within an hour from his call to her. He was still vague and non-descript on this call regarding how he came across the data in question. He told them he would contact Curtis (his boss) and would follow-up with them.
 - Feb. 9: Service Operations came to the Calverton office to fix the APG issue on the previous laptop. She and the IT Partner coordinated with the FCC to deliver the fixed/repaired laptop on 2/10.
 - Feb. 10: The IT partner was informed that the FCC OIG has informed FEC OIG that this represents a potential security breach. This same day, he goes with her to the FCC and they deliver the repaired laptop.
 - Feb. 10: The FEC OIG come to a meeting to pick up the laptop, and the FCC OIG gives a brief demo to show how he found the data in question on the laptop. The FEC also at this time copies the files onto another hard drive. FCC OIG shows his path to the data as “Start” – “Explore” – search through various profiles on the machine, and under one of the profiles, he finds an “[REDACTED] Old” directory under the “program files” within one of the profiles.
 - To date – FCC still has possession of both machines, as they refused to return the laptop in question (even though a repaired one with new APG and [REDACTED] loaded) due to wanted to swipe the machine of all data before returning. Auditor’s understanding is that to date, FCC still has possession of 2 CG laptops.
- Please describe your understanding of the nature and extent of FEC data that may have been disclosed/available from the laptop in question.

She stated she has never had any involvement in the FEC engagement. The only recollection she has of ever doing any work related to any FEC engagement was that she loaded an APG program into [REDACTED] in 2008. She was unaware of what the nature of the data would be – as her only exposure to the data was on the day that the FCC OIG showed how he found the files in question when CG delivered the repaired laptop.

- Do you have any direct or indirect knowledge of the laptop in question, including any employees who used the machine in the past, any other loan arrangements, any prior issues/problems with the machine that were reported or caused the machine to be sent back to technical support to re-image the machine, etc.?

She had no knowledge of how this [REDACTED] old” directory would have gotten onto the machine in question. Although, based on what she could piece together to date, she believed it would have been something left from when the subcontractor would have used it – as it appeared that these files were under his profile in the “Explore” tree that the FCC OIG had searched.

She is unaware and has no knowledge of ever even hearing of another situation like this during her time at CG.

She emphasized that it appeared as though this laptop hadn’t been accessed in a while, as the profile listed could not be used to log into the machine. Service Operations informed her that this was due to CG having controls to disable profiles after periods of inactivity. They then helped her to create a new profile in order to log in.

The only time she has had any involvement even similar regarding loaned laptops has been in her experience before with the FCC engagement and the loaned laptops.

She mentioned that she found it “odd” that the FCC OIG had asked her to review some specific [REDACTED] things with him on Feb. 2. In this meeting, which she said the FCC OIG requested, and took approximately 45 minutes... He inquired of her to show him details regarding how to search last saved/changed dates of [REDACTED] files. He also inquired about looking into the detail file structure of [REDACTED] directories and listings to see where these files load to, and how they show up in these directories (details, names, extensions, etc.).

- Do you have knowledge of a “post-it” note taped to the computer with account and password data? Why was this done, or did FCC OIG place this?

She acknowledged that it wasn’t good judgment to put the [REDACTED] account and password onto the laptop. However, it is her assertion that the only reason she put the password to the windows domain account was that the FCC OIG asked her what the new password was, and that he indicated it was OK for her to go ahead and write this on the note taped to the laptop as well. This information was then only documented along with the laptop at the consideration and in the presence of the FCC OIG contact.

- Do you have any direct or indirect knowledge of the laptop in question, including any employees who used the machine in the past, any other loan arrangements, any prior issues/problems with the machine that were reported or caused the machine to be sent back to technical support to re-image the machine, etc.?

No. Only person thought to have used it was a subcontractor on the FEC engagement in 2007.

Interview with IT Audit Manager (occurred on April 3):

During the interview with the IT Audit Manager, he indicated that he did not have any recollection of doing any work with, or having accessed the laptop in question. He asserted that he would not have had any contact with the machine based on his involvement with the subcontractor and the FEC engagement. While he wasn't completely clear initially as to whether he had received the engagement data from the subcontractor via CD or email; he was subsequently able to remember that he did receive the data through encrypted email transmissions and that he loaded the data into [REDACTED] from his own profile and laptop based on the emails provided.

Interview with three members of the MidAtlantic CSC (MACSC) Service Operations team (occurred Feb. 18):

The individual responsible for reformatting the drive in 2007, as well as the contact with whom the IT Senior spoke with when preparing the laptop for the FCC OIG were two of the three members present at the interview.

- What is the history of the laptop in question? Please review the history and elaborate on what engagements were involved with this machine, and which personnel had access to the computer. What is the timeline of these uses of the laptop, and whether the laptop was a prior employee machine, if it is part of a "loaner pool" of machines, etc.?

They confirmed the same set of events and timeline as discussed with the IT partner and Senior. They did not have any direct involvement/contact with the laptop in question during the timing of the events in question. The person who spoke with the senior indicated he had discussed how to reload a profile and how to load the [REDACTED] binder with her, but did not work with the machine directly. He also discussed with her how to delete the "recycle bin" and the other [REDACTED] binders on the laptop, but not how to re-image the drive, or delete other files on the machine.

They provided some documentation regarding when the machine was re-imaged in 2007 when given to the subcontractor, as well as documentation of when the machine was signed out to the senior from the secure storage area in [REDACTED], and documentation on a physical laptop inventory performed on 9/26/2008, when Service Operations documented that this laptop (via serial and asset tag #) were located in the secure area.

- Who was responsible for the loading of [REDACTED] engagement and data for the purposes of loaning this device to the OIG? Was any observation or confirmation of the process to prepare this device conducted?

The IT Senior prepared and loaded the [REDACTED] binder on the laptop. Service Operations was in contact during this process, though, and talked her through this over the phone, but was not directly involved in preparing this laptop.

- Do any internal procedures exist regarding the process for prepping devices that are to be on loan?

Yes. They did provide documentation on internal policies and procedures for transfers of computers, disposal, recycling, retention, and specific checklist procedures for disposal and for laptop setup for new and transferred machines.

Also, Microsoft SMS tool is used to track logons, and also helps to track inventory, as SMS has a baseline of machines, and tracks this via the logons to these machines through the network. If a machine is not logged into the network within 90 days, the network ID assigned to the machine is disabled. This is confirmed by the circumstances of this incident, as the senior could not login to the network with the laptop in question due to the period of inactivity with this machine exceeding 90 days, and the account had been disabled.

- Is there any evidence or documentation to support the tracking, procedures performed to prepare the device, and history of the chain of custody specific to the machine in question?

Yes. There is a workstation setup checklist prepared and signed as of 4/19/2007, checkout log to the senior in 2009 (2/2), and documentation of the inventory done in 9/26/2008 were provided to evidence some history of this machine and the chain of custody.

- What is the current status and possession of the laptop in question, and why?

FCC still maintains the device, as well as the other repaired laptop device. FCC and FEC have explained that they will release this once the data has been deleted and the investigations are concluded.

- Does the history of this machine include any erasing, swiping, or swapping of the hard drive? If so, please elaborate.

No record exists of it being returned by the subcontractor to the secure area and/or to Service Operations. However, in 4/19/2007, there was a reformat and reload of toolsets recorded on this machine by Service Operations.

- How is inventory of machines used in “loan” situations tracked and monitored?

SMS is used to track and monitor devices as the accounts logon to the network. This is monitored by the Service Operations group. The Service Operations manager tracks an excel spreadsheet of the laptops, where they are assigned to, who they are assigned to, etc. A technician, also in Service Operations, maintains an Access database to track laptop and device inventory, which has some more history built into the tracking. For “loaner” machines, there is also a tracking sheet in Calverton used to sign in/out machines in use for temp basis, for contractors, etc.

- Do you have ability to determine/track who has accessed the FEC engagement binder since 2004? Do you have any knowledge or monitoring of who has synchronized or downloaded any FEC data since 2004?

There is a process to monitor and identify who synchronized binders to the central file room either to their desktop and to [REDACTED]. It is unclear what level of detail of this log exists once a binder in “Finalized” in [REDACTED] status. For those “In Process” status, the detail logs are available. Service Operations will follow up with Corporate CG IT to determine what details and logs exist for FEC data engagements in [REDACTED].

- What physical security controls are applied to laptops stored as “pooled” machines or those returned by employees, or in various states or repair/replacement, etc.?

These machines are stored in locked/secure storage areas for both [REDACTED] and [REDACTED] offices. [REDACTED] is stored via a locked area with key and fob access. Those with access include office receptionists, as well as Service Operations, and also the PICs. For [REDACTED], office administrator, and Service Operations have keys to this area.

Interview follow-up with three members of the MidAtlantic CSC (MACSC) Service Operations team (occurred the week of Feb. 23):

An additional interview with the Service Operations was conducted the week of 2/23, based on additional information from the FEC OIG and other information obtained during the investigation.

- Who do laptops get returned to once CG determines that the machine is outdated?

CG purchases laptops. Once laptops are replaced or considered outdated (no specific requirement), CG will either donate the machines to charity, schools, or may allocate them to partners or employees in some situations for personal use.

- What other machines were used by the subcontractor?

Can't track machines he had prior to the documentation of April 2007. The current tracking and asset monitoring database process only went into place during late 2006 into early 2007. Further, the current database and tracking process for laptops only tracks the most recent possession. Simply stated, asset history is overwritten by whatever the most recent entry is. For example, if an employee's CG laptop is transferred to another

employee, the asset system would only have an entry for the current person in possession – not anything prior; although some additional details are kept in a backup copy of a spreadsheet used to support the database tracking.

Their understanding would be that no CG laptop would have been assigned to the subcontractor prior to 2007, as subcontractors used their own machines prior to the end of 2006 when CG began using [REDACTED].

- What logs are available to document the levels of synchronization and history of sync between the Central File Room server of [REDACTED] and local machines? What previous logs would exist on Evans engagement activity?

Engagements listed as “In Process” in [REDACTED] show up as having a synchronization history within the – Properties; Information; Advanced; Synchronization Log. Within this, there is some detail listing times and GID of the synchronization. However, once an engagement is closed or listed as “Finalized” this history information is not displayed.

Further, it was explained that there is likely no log of synchronizations with the subcontractor. This is due to the fact that subcontractor was not provided with a CG network ID. Therefore, he would not have been able to upload/sync data to [REDACTED] centrally. He would have needed to sync via a peer-to-peer connection with another persons laptop, or transferred files via email or CD. It is believed this may have taken place between the IT Audit Manager and the subcontractor.

- Does CG have capabilities or practices to swipe all machines, even those transferred internally? Auditors understanding is that the CG process is to reformat machines that are transfers and to only run “Kill Disk” to swipe drives in compliance with DoD standards when machines are to be sent to charity or re-allocated. FEC OIG had stated their specialists had indicated that laptops could be swiped for selective directories, etc. during internal transfers.

CG was not initially aware of this. CG only reformatted internally transferred machines. However – Effective 2/27/2009, the Director of Service Operations required that all machines returned to the “pool” or to the secure storage rooms will now be required to have the Kill Disk tool run against them to swipe the drives. On 3/2/2009, Service Operations informed the auditor that CG was investigating using [REDACTED] tools and capabilities to swipe selective directories/data during internal transfers.

- How did the subcontractor receive the laptop provided to him in April 2007? Was the machine new at that time?

Service Operations prepared a checklist for setting up and formatting the laptop to be used by the subcontractor on April 19, 2007. They indicated that at that time he would have provided it to someone in the Calverton office to provide to the subcontractor, that he did not provide it to him directly.

The purchase date of the laptop in question was determined to be 3/07/2005.

- Does HR or IT have a checklist for obtaining laptops and a checklist to follow for terminated/separated employees?

On 2/26/2009, HR provided a copy of the Termination checklist which is followed for employees. Since this was a subcontractor – no such form would have been used. However, again, the bottom of page 2 on this checklist includes a completion/requirement to return/obtain the computer, drives, cords, disks, etc.

The IT procedures for handling/receiving laptops from employees are listed in the IT Manual and within the Workstation standards.

- The data found was in a windows directory labeled “**████.old**” per FEC OIG. How would that have appeared is that standard naming, or was a directory created/renamed?

“Old” – would have been the name given to a backup copy of a binder/folder, and is to be removed per end user requirements to delete files/data from machines once engagements are finalized. Since this was listed under a separate profile in the directory – the process described to the senior over the phone would not have removed this.

Interview with the IT Partner (occurred on Feb. 13):

- Describe the nature of the circumstances and your understanding of the events and circumstances around this matter.

The FCC OIG was provided a laptop in August, 2008 for purposes of doing workpaper review on the IT portion of the FCC FISMA and CFO (Financial Statement) audits. In early Feb. (believed about 2/2), he reported that he could not access APG in order to review certain work steps. In order to expedite the request, the IT partner worked with the senior to get a computer from the █████ locked storage area, as apparently due to time constraints and concerns in the timing in his discussion with the FCC OIG, it was determined that returning the laptop through to the technical support group to fix and return would take too long.

The new laptop (the one in question) was then loaded with the █████ binder package for FCC, and all other █████ binders were deleted. This machine was delivered to the FCC OIG then on 2/2/2009. On Feb. 6, he reported that there was other data he could access on the laptop, reportedly related to the FEC.

In the meantime, he retained the prior laptop, had it fixed for APG, and reloaded with the updated █████ binder package for FCC. The repaired laptop was delivered to the FCC OIG on 2/10/2009. At that time, they refused to return the laptop in question, as he indicated they would not return until FCC OIG had an opportunity to delete all FCC data from the machine.

- Has any issue like this arisen in the past relative to loaned or shared laptops?

He indicated he had never experienced anything of this nature before in his time at CG. He articulated that the process of loaning these laptops for purposes of w/p review by the client is very rare, and only done for government projects – mostly with FCC.

- Is the use and loaning of this machine consistent with the nature of the engagement being done with the FCC? Do you have any knowledge to date of the nature or extent or type of data in question that may have been disclosed relative to clients/agencies outside of the FCC?

His understanding is that the FCC has done w/p review like this in the past, but was never an issue before. The understanding to date is that they don't believe there is PII data, but some data of an IT nature that may be considered confidential and sensitive. This laptop was isolated to only being given to another federal government employee of the OIG office (FCC) and to date believe it only contained a backup engagement and files for an FEC audit.

- What employees have participated in the FEC engagements since 2004, including any temporary employees, contractors, interns, terminated employees, etc.?

Would need to run a “Time21” report to determine employees who charged hours to the FEC. Will need to obtain additional input to determine what contractors may have participated in FEC engagements. (This data was subsequently obtained and reviewed by the Auditor).

- Are you aware of a “post-it” note taped to the laptop in question with account and password data on it? Why was this done?

His understanding was that the password for the account was written on the laptop in the presence of the FCC OIG per discussion and request with/from him. There is acknowledgement that having this post-it with any information was not a good judgment or practice.

He inquired whether/why the FCC OIG would not have removed this. Auditor will inquire of the FCC OIG on this matter, as well as to what procedures/responsibilities are outlined in “acceptable usage” with the OIG when in possession of CG equipment/devices. [Based on additional follow-up and determinations – questions were not specifically directed by the Auditor to the FCC OIG due to statements from FCC OIG, as well as the protocols and requirements indicated by the FCC OIG to address questions].

- The data in question is sensitive IT data. Can you describe the need/purpose of including this data within the w/p detail for this engagement?

The IT partner indicated that FISCAM and other guidance specifically indicate the value and purpose of obtaining and reviewing network diagrams and related network/infrastructure documentation. Given that this was a financial statement audit

(not FISMA), the IT partner acknowledged that the IP addresses and machine name details were likely not necessary, but that this type of data is typically obtained as part of FISMA engagements. The discussion included the fact that network diagrams are often obtained and provide significant value for financial audits (CFO) to determine the nature of the IT environment, extent of application and database servers, to validate the Primary Domain Controller and Backup Domain Controller (PDC and BDC) to be reviewed/tested, etc. The consensus was that while network diagrams and related data are needed for financial audits, the IP addresses, machine names, and similar level of sensitive details and/or account and password data should be redacted before inclusion in the detail w/p's, or returned/destroyed after final w/p review.

- Describe the “chain of custody” of the laptop at the time it was provided by technical support until when it was delivered to the client.

Tech support not involved with this laptop. The IT Senior and Calverton office secretary/manager involved in taking machine out of storage closet, signing it out, and coordinating only over the phone with tech support to get binder package loaded and other binders deleted (through). Machine then delivered to the FCC OIG.

- Please describe your understanding of the nature and extent of FEC data that may have been disclosed/available from the laptop in question.

Unknown exactly at time of interview. Believed not to be PII, but maybe some sensitive data. Auditor confirmed with FEC OIG and FEC CIO and CISO that data in question was not PII, and that it was related to IP addresses and confidential password and/or other system data.

- Do you have any direct or indirect knowledge of the laptop in question, including any employees who used the machine in the past, any other loan arrangements, any prior issues/problems with the machine that were reported or caused the machine to be sent back to technical support to re-image the machine, etc.?

No. Only person thought to have used it was a subcontractor on the FEC engagement in 2007.

Interview follow-up with the IT Partner (occurred on March 9):

An additional interview with the IT Partner was held on 3/9. This was due to obtaining clarifications from additional information obtained during the procedures.

- Did the subcontractor use his own machine or the company provided laptop prior to 2007 for subcontracting engagements?

Used his own SamLin machine prior to 2007. 2007 was the first year CG did the IT procedures for FEC, as this coincides with the RAS standards from SAS's and application

to Federal clients. Prior to 2007, workpapers were done in electronic form and stored on the G:/ drive of the network, and prior to 2005 – work was done in paper copy.

- Did the subcontractor have a UserID to the network? Service Ops indicates that he did not, and therefore would have done all synchronization on a peer-to-peer or other basis to update engagement binders/files. Did he synchronize with the IT Manager or someone else?

No access given to subcontractors for the network. He was not sure how exactly the subcontractor synched his data to the [REDACTED] engagement file and central file room. The IT Manager had informed him that he didn't specifically recall either exactly how he received the data from the subcontractor.

- How did the subcontractor receive the laptop in 2007? Service Operations indicated that they provided this to someone in the Calverton office. Was the IT Manager or someone else involved in actually providing the machine?

He believed this would have been either the Audit Manager or the IT Manager. It was later clarified by the Auditor that this was the FEC Audit Manager who personally transferred/delivered the laptop.

- Do we require subcontractors to sign a policy for acceptable use, handling of CG provided laptops, etc.? Do they sign acknowledgement of receipt of the machine, etc.?

No. Not aware of anything.

- Do we have a contract with SamLin to date back to 2004, or at least for 2007?

Not aware of anything, and still has not located a copy of a contract to date. The Auditor later clarified with the Calverton PIC that a contract does exist – but that the FEC engagement specifically is not listed.

- Can you estimate when this machine would have been returned in late 2007/early 2008?

Believes it was the fall of 2007.

Interview with the Subcontractor and subcontractor Firm owner (occurred on March 10 – follow up calls also took place the week of 3/16 to confirm that FEC data had been deleted from SamLin machines):

- How did you sync your FEC data to [REDACTED] engagement in 2007? Do you have any knowledge of this “[REDACTED].old” file?

[REDACTED] was loaded onto a computer for the first time in 2007. They have no indication as to what this “[REDACTED].old” file was. Subcontractor did not load any actual data onto the CG laptop, as he had continual issues/problems with uploading the data he had into [REDACTED] on the CG

laptop. Therefore, he provided his data to the IT Manager via an encrypted zip file through email. The owner confirmed this, as he stated he recalled the upload problems and seeing the emails with the sent encrypted file. Subcontractor indicated he believed some data was already loaded into [REDACTED] engagement, but he thought everything was within [REDACTED]... he was not aware of any data loaded outside of [REDACTED] engagement.

- Did you ever use your personal email address/account to send data that was business related regarding the FEC?

Yes, vt.edu address was used on the first year of the engagement only (2004) and was addressed with the FEC CIO and the FEC at the time. Later that year, as well as in the 2005 engagement, he used his SamLin Consulting email address. Starting in 2006, he indicated that the FEC required the use of their approved email accounts for business purposes.

- Did you ever use 2 laptops during your employ with CG? Was one a personal laptop? Did you ever use your personal laptop for business purposes, including copying, creating, emailing, etc. any files related to FEC?

A personal laptop was never used. He used his SamLin laptop during his tenure on the engagement. In 2007 was the first year that he also used a CG machine, as this was provided so he could upload his files onto a local copy of [REDACTED] onto that machine. This upload didn't work, which may have led to the issue of the backup copy of [REDACTED] data.

He did have engagement data loaded onto his own machine from SamLin, as well. Auditor later confirmed with subcontractor and the firm's owner that this data had been deleted, except for the narrative write-ups drafted by the subcontractor.

- When were you involved in doing FEC related engagements on behalf of CG?

Since 2004.

- Have you ever shared/disclosed any FEC data outside of FEC management, OIG, or other CG personnel?

No. Auditor has noted though, per previous questions, that he did load and put FEC data on his SamLin provided laptop also.

- Who gave you the CG laptop in 2007?

The Audit Manager provided him the computer. He noted that he received the laptop from her in June 2007.

- Whom did you return your laptops to after your periods of subcontracting/employment with CG?

He returned the machine to the Audit Manager, as well.

- Were you asked to sign anything at CG regarding confidentiality, accepted usage of CG laptops, etc.?

He signed an NDA and Security Awareness verification with the FEC, but did not sign anything specific with CG. The owner also signed an NDA.

- What other engagements outside of FEC did you work on during your time working on behalf of CG?

None. They both stated that the subcontractor did not participate on any other CG related engagements during the time he worked on FEC.



Federal Communications Commission
Office of Inspector General
445 12th Street, S.W.
Washington, D.C., 20554

(202) 418-0470 VOICE
(202) 418-2811 FAX

Fax

To: Joe Duncan **From:** [REDACTED] FCC OIG

Company: FEC OIG **Date:** May 11, 2009

Fax: (202) 501-8134 **Pages:** 3

Phone: (202) 694-1316

Re: Log Screen Shots

Urgent **For Review** **Please Comment** **Please Reply** **Please Recycle**

● **Comments:**

```

=== Verbose logging started: 3/8/2008 10:22:05 Build type: SHIP UNICODE 3.01.4000.2435 Calling process:
C:\WINDOWS\system32\msiexec.exe ===
MSI (c) (60:74) [10:22:05:719]: Resetting cached policy values
MSI (c) (60:74) [10:22:05:719]: Machine policy value 'Debug' is 0
MSI (c) (60:74) [10:22:05:719]: ***** RunEngine:
***** Product: \\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for PC.msi
***** Action:
***** CommandLine: *****
MSI (c) (60:74) [10:22:05:719]: Client-side and UI is none or basic: Running entire install on the server.
MSI (c) (60:74) [10:22:05:719]: Grabbed execution mutex.
MSI (c) (60:74) [10:22:06:160]: Cloaking enabled.
MSI (c) (60:74) [10:22:06:160]: Attempting to enable all disabled privileges before calling Install on Server
MSI (c) (60:74) [10:22:06:170]: Incrementing counter to disable shutdown. Counter after increment: 0
MSI (s) (18:30) [10:22:06:610]: Grabbed execution mutex.
MSI (s) (18:7C) [10:22:06:610]: Resetting cached policy values
MSI (s) (18:7C) [10:22:06:610]: Machine policy value 'Debug' is 0
MSI (s) (18:7C) [10:22:06:610]: ***** RunEngine:
***** Product: \\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for PC.msi
***** Action:
***** CommandLine: *****
MSI (s) (18:7C) [10:22:07:031]: Incrementing counter to disable shutdown. Counter after increment: 0
MSI (s) (18:7C) [10:22:07:282]: Machine policy value 'DisableUserInstalls' is 0
MSI (s) (18:7C) [10:22:08:233]: File will have security applied from OpCode.
MSI (s) (18:7C) [10:22:18:803]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied. Counter
after decrement: -1
MSI (s) (18:7C) [10:22:18:803]: SOFTWARE RESTRICTION POLICY: verifying package -->
'\\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for PC.msi' against software restriction policy
MSI (s) (18:7C) [10:22:18:803]: SOFTWARE RESTRICTION POLICY: \\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for
PC.msi has a digital signature
MSI (s) (18:7C) [10:22:42:037]: SOFTWARE RESTRICTION POLICY: \\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for
PC.msi is permitted to run at the 'unrestricted' authorization level.
MSI (s) (18:7C) [10:22:42:207]: End dialog not enabled
MSI (s) (18:7C) [10:22:42:207]: Original package ==> \\cgebiz.net\dfs\SMSInstall\wm\PointSec\62HF1\Pointsec for PC.msi
MSI (s) (18:7C) [10:22:42:207]: Package we're running from ==> C:\WINDOWS\Installer\4a1ce.msi
MSI (s) (18:7C) [10:22:43:520]: APPCOMPAT: looking for appcompat database entry with ProductCode
'{31B33270-24D7-4307-84F2-A3288636B83A}'.
MSI (s) (18:7C) [10:22:43:700]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (18:7C) [10:22:43:790]: MSCOREE not loaded loading copy from system32
MSI (s) (18:7C) [10:22:44:461]: Machine policy value 'TransformsSecure' is 1
MSI (s) (18:7C) [10:22:44:522]: Machine policy value 'DisablePatch' is 0
MSI (s) (18:7C) [10:22:44:522]: Machine policy value 'AllowLockdownPatch' is 1
MSI (s) (18:7C) [10:22:44:522]: Machine policy value 'DisableLUAPatching' is 0
MSI (s) (18:7C) [10:22:44:562]: Machine policy value 'DisableFlyweightPatching' is 0
MSI (s) (18:7C) [10:22:44:732]: APPCOMPAT: looking for appcompat database entry with ProductCode
'{31B33270-24D7-4307-84F2-A3288636B83A}'.
MSI (s) (18:7C) [10:22:44:732]: APPCOMPAT: no matching ProductCode found in database.
MSI (s) (18:7C) [10:22:44:732]: Transforms are not secure.
MSI (s) (18:7C) [10:22:44:792]: Command Line: REBOOT=ReallySuppress CURRENTDIRECTORY=S:\wm\PointSec CLIENTUILEVEL=3
CLIENTPROCESSID=2656
MSI (s) (18:7C) [10:22:44:802]: PROPERTY CHANGE: Adding PackageCode property. Its value is
'{9DBEC128-3BAC-4AA9-9A40-A3EC13DB80F8}'.
MSI (s) (18:7C) [10:22:44:802]: Product Code passed to Engine.Initialize:

```

C: pointsecinstall.log - Notepad

File Edit Format View Help

```

Property(S): PROGMSG_IIS_REMOVEAPPPOLS = Removing application pools...
Property(S): PROGMSG_IIS_REMOVEWEBSERVICEEXTENSION = Removing web service extension
Property(S): PROGMSG_IIS_REMOVEWEBSERVICEEXTENSIONS = Removing web service extensions...
Property(S): PROGMSG_IIS_ROLLBACKAPPPOLS = Rolling back application pools...
Property(S): PROGMSG_IIS_ROLLBACKWEBSERVICEEXTENSIONS = Rolling back web service extensions...
Property(S): DWJSLINK = CE4C00D80E2BB75FCEACA758CEEC978FDEFC008FCEBC879FCE7BB728D98CA7DF3E3CB7CF9EAC
Property(S): ARPURLINFOABOUT = http://www.checkpoint.com
Property(S): ARPNOMODIFY = 1
Property(S): ARPNOREPAIR = 1
Property(S): REMOVEPOINTSEC = 0
Property(S): SHOWLAUNCHPROGRAM = 0
Property(S): REBOOT = Reallysuppress
Property(S): REG_EXTEND_LOGGING = 0
Property(S): REG_LOG_TRANSFER = 1
Property(S): RestartManagerOption = CloseRestart|
Property(S): REG_LANGUAGE = XX
Property(S): POINTSEC_DLL_LOADED = 0
Property(S): REGINSTALLTIME = 1204990230
Property(S): PointsecDummyReturn = 0
Property(S): REGALLUSERSPROFILE = C:\Documents and settings\All Users\Application Data\Pointsec\pointsec for PC\
Property(S): REG_MAX_LOG_TRANSFER_MAX_SIZE = 10
Property(S): REG_SHOW_RECOVERY_MESS = 0
Property(S): ARPINSTALLLOCATION = C:\Program Files\Pointsec\Pointsec for PC\
Property(S): PointsecDLLPath = C:\DOCUME~1\whit6274\LOCALS~1\Temp\{31B33270-24D7-4307-84F2-A3288636B83A}
Property(S): RemoteAdminTS = 1
Property(S): MsINTProductType = 1
Property(S): ServicePackLevelMinor = 0
Property(S): ServicePackLevel = 2
Property(S): windowsBuild = 2600
Property(S): VersionMsi = 3.01
Property(S): VersionDatabase = 200
Property(S): CLIENTPROCESSID = 2656
Property(S): CLIENTUILEVEL = 3
Property(S): COMPANYNAME = Clifton Gunderson
Property(S): USERNAME = Clifton Gunderson
Property(S): CURRENTDIRECTORY = S:\wm\PointSec
Property(S): PackageCodeChanging = 1
Property(S): ProductState = -1
Property(S): PackageCode = {9D8EC128-3BAC-4AA9-9A40-A3EC13DB80F8}
Property(S): ProductToBeRegistered = 1
MSI (s) (18:7C) [10:32:12:750]: Note: 1: 1707
MSI (s) (18:7C) [10:32:12:750]: Product: Pointsec PC -- Installation operation completed successfully.

MSI (s) (18:7C) [10:32:12:870]: Cleaning up uninstalled install packages, if any exist
MSI (s) (18:7C) [10:32:12:910]: MainEngineThread is returning 0
MSI (s) (18:30) [10:32:13:011]: Destroying RemoteAPI object.
MSI (s) (18:20) [10:32:13:251]: Custom Action Manager thread ending.
=== Logging stopped: 3/8/2008 10:32:12 ===
MSI (c) (60:74) [10:32:13:251]: Decrementing counter to disable shutdown. If counter >= 0, shutdown will be denied. counter
after decrement: -1
MSI (c) (60:74) [10:32:13:251]: MainEngineThread is returning 0
=== Verbose logging stopped: 3/8/2008 10:32:13 ===
    
```

FOIA 2016-32_349 TOTAL P. 03

MHY-11-2009 15:45 FCU UIA 202 419 2811 P. 03

**FEDERAL ELECTION COMMISSION
OFFICE OF INSPECTOR GENERAL**



Report of Investigation

Hatch Act Violations

Case Number INV-13-04

June 25, 2014

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General, and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission, or designee. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

Table of Contents

	<u>Page</u>
I. Executive Summary	1
II. Investigation Details	2
A. Criminal Solicitation	3
B. Ethics Violations Predicated Upon The Webcast	4
C. Ethics Violations Predicated Upon Twitter Activity	5
D. OSC Settlement Agreement	6
E. Termination of the Investigation	7
III. Findings	7
IV. Suggestions	7
V. Background	8
A. Relevant Statutes, Regulations and Policies	8
B. Scope of the Investigation	9
VI. Privacy Act and Freedom of Information Act Notice	9
Attachment List	10

I. Executive Summary

On November 1, 2013, the [REDACTED] notified the Office of Inspector General (OIG) that on October 24, 2013, the Office of General Counsel (OGC) had made a referral to the Office of Special Counsel (OSC) concerning OGC [REDACTED] attorney [REDACTED] [REDACTED] who they discovered had made several tweets or re-tweets (forwarded tweets originated by another user) that appeared to violate the Hatch Act.¹ These tweets expressed support and solicited contributions for the election of certain Democratic candidates for Federal office, including President Barack OBAMA, Cory BOOKER and Wendy DAVIS. The referral states that [REDACTED] was considered a “further restricted” employee under the Hatch Act.²

The OIG initiated a joint investigation with the OSC’s Hatch Act Unit. The OSC was to investigate and prosecute the alleged Hatch Act violations, and the OIG was to investigate any criminal, ethics, or administrative violations, including misuse of government property and misuse of official time. The OIG would also issue the necessary subpoenas and coordinate the computer forensic analysis of [REDACTED] FEC-issued computer. Due to the potential criminal violation of 18 U.S.C. § 607, soliciting political contributions from a building occupied in the discharge of official Federal duties, the Public Corruption Unit of the USAO was notified.

During the investigation, the OIG obtained information that [REDACTED] participated on a panel discussing 2012 Republican presidential candidate Mitt ROMNEY that was broadcast live over the internet via the Huffington Post website (the “webcast”). During the webcast, [REDACTED] made negative comments about ROMNEY and Republicans in general. [REDACTED] participation in the webcast constituted misuse of government property, misuse of official time, and violated a requirement for FEC employees to obtain prior approval for certain outside activities related to their official duties.

Records from WebTA, the FEC’s time and attendance program, show [REDACTED] was working from the FEC building the day of the webcast, and FEC Office of the Chief Information Officer (OCIO) records show [REDACTED] reserved the FEC computer training room in the FEC building for a two hour period covering the time of the live broadcast. The wall and chair rail visible behind [REDACTED] in the webcast are identical to those in the computer training room. The training room computers are equipped with Logitech webcams and enabled to support web video conferencing. The training room computers had been replaced, wiped, and returned to the General Services Administration as surplus between the time of the webcast and the time they were examined by OCIO personnel, so

¹ The Hatch Act, 5 U.S.C. § 7321-6, prohibits Federal employees from engaging in specified political activities.

² The FEC is one of several enumerated agencies whose employees have further political activity restrictions, in addition to those restrictions covering all Federal employees, placed upon them by the Hatch Act. 5 U.S.C. § 7323(b)(1), (2).

their internet histories did not go back far enough to yield any results from a search for the webcast activity.

On April 2, 2014, a settlement agreement between [REDACTED] and the OSC was executed. In the agreement, [REDACTED] admitted to violating the Hatch Act by [REDACTED]. [REDACTED], agreed to resign from the FEC, and agreed to a two-year debarment from Federal employment. ([REDACTED]).

Pursuant to the terms of the settlement agreement, on April 4, 2014, [REDACTED] tendered [REDACTED] resignation from the FEC, which became effective April 5, 2014.

As [REDACTED] is no longer an employee of the FEC, the FEC has no jurisdiction to impose administrative sanctions, including disciplinary and adverse actions, upon [REDACTED]. The USAO issued a declination of prosecution on June 3, 2014. Therefore, the OIG concluded its investigative work in this matter on June 3, 2014.

The OIG will conduct a separate inquiry to determine whether there is any evidence of political bias in [REDACTED] cases to which [REDACTED] was assigned. [REDACTED] was assigned to a [REDACTED], and did not work directly on [REDACTED] cases after that date. While on the special projects team, however, [REDACTED] was assigned to draft four (4) reports recommending to the Commission complaints that did not meet certain established thresholds be dismissed; [REDACTED] had no discretion in these assignments.

II. Investigation Details

This matter was initiated on November 1, 2013, when the OIG received a telephonic hotline complaint from [REDACTED]. According to [REDACTED], on October 24, 2013, the OGC had made a referral to the OSC concerning [REDACTED] Twitter activity that appeared to violate the Hatch Act.³ A copy of the OGC's referral to the OSC was forwarded to the OIG. Attachment 1. The OIG

³ 5 C.F.R. § 704.102(a) provides the OSC with exclusive jurisdiction to investigate and prosecute Hatch Act violations. However, the Inspector General Act of 1978, as amended (IG Act) makes it an IG's statutory "duty and responsibility" to investigate matters "relating to the programs and operations" of the agency. For most Federal agencies, Hatch Act violations may not relate directly to the programs and operations of the agency, with some exceptions. The FEC, though, is tasked with, *inter alia*, the regulation and enforcement of Federal political campaign activity and organizations, which creates a relationship between a Hatch Act violation by an FEC employee and the programs and operations of the FEC. Therefore, Hatch Act violations fall within the OIG's statutory jurisdiction, and the OSC has concurrent jurisdiction. A misunderstanding of this joint jurisdiction may have partially contributed to the short delay in reporting the matter to the OIG after it had been reported to the OSC.

immediately contacted the OSC's Hatch Act unit to initiate a joint investigation, and OIG personnel met with representatives from the OSC's Hatch Act Unit on November 6, 2013. Training records show ██████ a FEC ██████ attorney since ██████, had received Hatch Act training in 2010 and 2012. Attachment 2.

Subpoenas were issued to Twitter for ██████ two known accounts, with the usernames ██████ and ██████. Information was developed during the search of ██████ Lotus Notes email account that ██████ established a Logitech, Inc., account on the day of and just prior to the webcast, and likely used a Logitech video conferencing system to participate in the webcast; therefore, a subpoena was issued to Logitech. Twitter and Logitech both produced the information requested to the extent they possessed or controlled it. Information related to the webcast was also sought from AOL, Inc., parent company of the TheHuffingtonPost.com, Inc., HuffPost News and HPMG News (collectively AOL). AOL provided the information without a subpoena, as some of it was generally publicly available.

██████ FEC-issued computer was seized and turned over to the Computer Crimes Unit of the United States Postal Service OIG (USPS OIG) for forensic analysis, including a hard drive search. The OCIO was enlisted to assist with the capture of ██████ FEC Lotus Notes email account and in tracking ██████ use of FEC computer equipment. ██████ WebTA and Hatch Act training records were obtained from the FEC OGC.

Due to the potential criminal violation of 18 U.S.C. § 607, soliciting political contributions from a building occupied in the discharge of official Federal duties, the Public Corruption Unit of the USAO was notified. In addition to the USAO, coordination and advice was also sought from the Election Crimes Branch of the Public Integrity Section and the Computer Crimes and Intellectual Property Section of the Department of Justice (collectively, with the USAO, DOJ). The DOJ was kept apprised of all proposed investigative actions, including the workplace and email searches, computer forensic analysis, proposed subpoenas and other information gathering activities.

A. Criminal Solicitation

While Federal employees engaging in specified political activities while on duty or in a Federal building and soliciting political contributions either on or off duty constitute administrative violations of the Hatch Act and ethics regulations, soliciting political contributions from inside a Federal building is also a criminal offense. The OSC provided information to the OIG showing dates and times when ██████ made apparent solicitations for political contributions to candidates for Federal elections through ██████ Twitter account. The OSC noted, however, that there were discrepancies with the time stamps on printouts of ██████ tweet from the Twitter website. An initial OIG review compared the OSC information to ██████ WebTA records, and several of the solicitations appeared to have been made on dates when ██████ was working at the FEC building

at 999 E Street, Northwest, Washington, DC 20463 (FEC building). The FEC building is used and occupied by Federal employees in the discharge of official duties.

Although [REDACTED] tweeted solicitations on dates when [REDACTED] worked, a review of the available information was unable to place [REDACTED] inside the FEC building at the exact times of the solicitations. The timestamps on the printouts from Twitter's public website were unreliable due to the discrepancies noted by OSC, thus the printouts could not be used to determine the exact times of the solicitations. Therefore, either an analysis of records subpoenaed from Twitter or a computer forensic analysis of [REDACTED] FEC-issued computer was needed to place [REDACTED] in the FEC building at the times of the solicitations,

It was anticipated that the dates and times contained in the internal records subpoenaed from Twitter would be more accurate than those on the public website printouts. The subpoena also requested records of the Internet Protocol (IP) addresses of the computers [REDACTED] used for the solicitations, which would have revealed if [REDACTED] had used [REDACTED] FEC-issued computer to make the solicitations. However, the information produced by Twitter in response to the subpoena did not go back far enough in time to show the dates and times of the solicitations or capture the IP addresses of the computer devices used by [REDACTED] for the solicitations, as this information was apparently not retained by Twitter. The forensic analysis of [REDACTED] FEC-issued computer was not helpful in determining whether [REDACTED] used government property for the solicitations because, according to the OCIO, [REDACTED] computer had been replaced as part of the normal replacement cycle between the dates of the solicitations and the date it was seized.

The USAO issued a declination of prosecution on June 3, 2014, based primarily on the lack of information to place [REDACTED] inside the FEC building at the times of the solicitations. Although [REDACTED] separately admitted to [REDACTED] [REDACTED] did not specifically admit to soliciting while inside the FEC building. Attachment 1.

B. Ethics Violations Predicated Upon The Webcast

The webcast was not mentioned in the OGC's referral to the OSC or the OIG and was discovered during the course of the OIG investigation. The OIG obtained information that [REDACTED] participated in the webcast on [REDACTED] 2012, at 12:00 p.m. Eastern Standard Time. [REDACTED] image and voice appeared on a HuffPost Live "Community Sound Off" audio-video webcast, moderated by Ahmed Shihab-Eldin, titled "Ann Romney to Mitt Critics - 'Stop It,'" and broadcast live over the internet to the public, as a member of a panel discussing the 2012 presidential campaign. [REDACTED] name, occupation (lawyer), and location (Washington, DC) were mentioned by the moderator and appeared on the screen when [REDACTED] spoke, as did [REDACTED] Twitter username, [REDACTED] Attachment 3. During the webcast, [REDACTED] made negative comments about ROMNEY, and Republicans in general. For example, [REDACTED] made a comment that appeared to be

directed to ROMNEY or ROMNEY's wife, Ann, or both, that they needed to "grow a backbone" in response to Ann ROMNEY's complaints about criticism of [REDACTED] husband. [REDACTED] also stated that the ROMNEY campaign was "making excuses," and that it was "reflective of the entire Republican platform."

WebTA records show [REDACTED] was working from the FEC building that day, and OCIO records show [REDACTED] reserved the FEC computer training room in the FEC building for a two hour period covering the time of the live broadcast. Attachment 4. The wall and chair rail visible behind [REDACTED] in the webcast are identical to those in the computer training room. The training room computers are equipped with Logitech webcams and enabled to support web video conferencing. The training room computers had been replaced between the time of the webcast and the time they were examined by OCIO personnel, so their internet histories did not go back far enough to yield any results from a search for the webcast activity.

Under the Hatch Act statute and regulations, a Federal employee is prohibited from engaging in political activity, which is defined as an activity directed toward the success or failure of political party or candidate for partisan political office, while on duty and in any room or building occupied in the discharge of official duties.⁴ In the settlement agreement, [REDACTED]

[REDACTED] Attachment 5. [REDACTED] resulted in a misuse of Government property pursuant to 5 C.F.R. § 2635.704, and constituted a misuse of official time pursuant to 5 C.F.R. § 2635.705.

A review of records by the Deputy DAEO found that [REDACTED] had not sought prior approval to participate in the webcast. Prior approval was required because, under 5 C.F.R. § 4701.102, the webcast participation was an uncompensated activity by providing services as a speaker. Further, [REDACTED] comments about ROMNEY, the ROMNEY campaign, and the Republican Party in general, pertained to matters involving an "ongoing or announced Commission policy, program, or operation," because the FEC was involved in the administration and enforcement of Federal election campaign laws involving these parties at the time of the webcast.

C. Ethics Violations Predicated Upon Twitter Activity

Apart from [REDACTED] participation in the webcast, [REDACTED] admitted in the settlement agreement to [REDACTED]. Committing a Hatch Act violation by engaging in political activity within the FEC building, while

⁴ 5 U.S.C. §§ 7324(a)(1), (2); 5 C.F.R. §§ 734.306(a)(1), (3).

⁵ For purposes of the Hatch Act, "on duty" means "in a pay status other than paid leave, compensatory time off, credit hours, time off as an incentive award, or excused or authorized absence (including leave without pay)." 5 C.F.R. § 734.101.

on duty, or through the use of a government computer, constitutes a misuse of Government property and a misuse of official time.

The OIG had planned to obtain evidence of discrete misuse of government property and official time violations related to [redacted] Twitter activity by conducting a review of OSC’s Hatch Act analysis, in conjunction with other information, such as WebTA records and computer forensic results. Both the subpoena response from Twitter and the computer forensic analysis provided evidence, in the form of IP addresses used and the hard drive analysis, that [redacted] used [redacted] FEC-issued computer to access and use [redacted] Twitter account. [redacted] settlement agreement, however, abrogated further action and analysis related to [redacted] Twitter activity. Therefore, while the Hatch Act violations that [redacted] admitted to [redacted] constitute a misuse of government property and official time in general, the specific circumstances of each violation were not detailed.

D. OSC Settlement Agreement

[redacted]

E. Conclusion of Investigative Activity

█████ submitted █████ SF-52 resignation form on April 4, 2014, with an effective date of April 5, 2014. Investigative activity concerning ethics violations by █████ ceased when █████ submitted █████ resignation, as this action removed the FEC's ability to impose administrative sanctions, but investigative activity concerning potential criminal violations by █████ continued until the USAO issued a declination of prosecution on June 3, 2014. The OIG had anticipated conducting with the OSC a joint interview of █████ but the settlement occurred prior to the interview being attempted.

As mentioned previously, the OIG will conduct a separate inquiry to determine whether there is any evidence of political bias in Enforcement Division cases to which █████ was assigned

III. Findings

█████ admitted to Hatch Act violations by █████. Based on these admissions, █████ misused Government property in violation of 5 C.F.R. § 2635.704 and misused official time in violation of 5 C.F.R. § 2635.705.

█████ violated 5 C.F.R. § 4701.102 by not seeking or receiving approval to participate in the webcast.

IV. Suggestions

Based on these findings, the OIG suggests that management consider the following:

- The Commission should consider promulgating a broadly worded directive to prohibit employees from using any FEC property or facilities for any partisan or political purpose, including providing commentary meant to be disseminated to the general public on matters before or over which the Commission has jurisdiction, to capture activity that might otherwise fall outside current statutes and regulations.
- The Commission should explore revising its supplemental ethics regulations or issue new regulations to expressly address providing commentary meant to be published, broadcast, or otherwise disseminated to the general public on matters before or over which the Commission has jurisdiction, taking into account employees' First Amendment protections.

V. Background

A. Relevant Statutes, Regulations and Policies⁶

18 U.S.C. § 607(a): It is a crime for anyone who is an officer or employee of the United States government, “to solicit or receive a donation of money or other thing of value in connection with a Federal, State, or local election, while in any room or building occupied in the discharge of official duties by an officer or employee of the United States, from any person.”

5 C.F.R. § 2635.704(a): An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.⁷

5 C.F.R. § 2635.705(a): Unless authorized in accordance with law or regulations to use such time for other purposes, an employee shall use official time in an honest effort to perform official duties.

5 C.F.R. § 4701.102:

(a) Definitions. For purposes of this section:

....

(3) Definition of outside employment. For purposes of this section, outside employment means any form of non-Federal employment, business relationship or activity involving the provision of personal services, whether or not for compensation. It includes, . . . , speaker, writer, or any other services provided by an individual.

(4) Related to the employee's official duties means that the outside employment meets one or more of the tests described in 5 C.F.R. §§ 2635.807(a)(2)(i)(B) through (E). Outside employment related to the employee's official duties includes:

....

(iv) Outside employment that deals in significant part with any matter to which the employee is or has been officially assigned in the last year, or any ongoing or announced Commission policy, program, or operation.

(b) Prior approval requirement. An employee of the Commission, . . . , shall obtain written approval from the Designated Agency Ethics Official before engaging in outside employment where the services provided:

⁶ The Hatch Act statute and regulations are not addressed in this section because the OIG and the OSC agreed that the OSC would be responsible for investigating [REDACTED] alleged Hatch Act violations. However, Hatch Act statutes and regulations form the basis for some of the ethics violations investigated by the OIG.

⁷ While FEC Directive 58 allows for *de minimis* personal use of FEC-issued computers, such permitted use does not extend to use that violates statutes or regulations, as such use is by its nature unauthorized, or where it impedes fulfillment of FEC work. Thus, using a government computer to commit a Hatch Act violation is not an “authorized purpose” under section 2635.704, regardless of a *de minimis* personal use policy.

(1) Are related to the employee's official duties

B. Scope of the Investigation

The investigation was limited to [REDACTED] activities. There was no indication any other FEC or Federal employee was involved in the activities described in this report. This report is limited to the purported criminal and ethical violations by [REDACTED] as the OSC was tasked with the analysis and report of [REDACTED] Hatch Act activity, except for when the Hatch Act violations inform the criminal and ethics violations.

VI. Privacy Act and Freedom of Information Act Notice

This report is the property of the Office of Inspector General, and is for OFFICIAL USE ONLY. Appropriate safeguards should be provided for the report, and access should be limited to Federal Election Commission officials who have a need-to-know. All copies of the report have been uniquely numbered, and should be appropriately controlled and maintained. Public disclosure is determined by the Freedom of Information Act, 5 U.S.C. § 552a. In order to ensure compliance with the Privacy Act, this report may not be reproduced or disclosed outside the Commission without prior written approval of the Office of Inspector General.

ATTACHMENTS

Attachment	Description
1	Referral from OGC to the OSC, dated October 24, 2013
2	Hatch Act Training Rosters for 2010 and 2012
3	Screen capture of [REDACTED] participation in the webcast
4	[REDACTED] WebTA record and computer training room reservation for September 21, 2012
5	[REDACTED]

Attachment No. 1

Referral from OGC to the OSC
dated October 24, 2013

Case Number INV-13-04



FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

October 24, 2013

Via E-Mail and First-Class Mail

Ana Galindo-Marrone, Chief
Leslie Gogan
Hatch Act Unit
Office of Special Counsel
1730 M Street NW, Suite 218
Washington, D.C. 20036-4505

Re: Hatch Act Referral – [REDACTED] FEC Attorney

Dear Ms Galindo-Marrone and Ms. Gogan:

By this letter, I am referring to you for whatever action the Office of Special Counsel may deem appropriate potential violations of the Hatch Act, 5 U.S.C. § 7321 *et seq.*, by [REDACTED], an attorney in the [REDACTED] of the Office of General Counsel of the Federal Election Commission ("OGC"). [REDACTED] has been an employee of the Commission since [REDACTED]. As an FEC employee, [REDACTED] is a "further-restricted" federal government employee under the Hatch Act. *See* 5 U.S.C. § 7323(b)(2) and (3).

As described more specifically below, it appears that [REDACTED] may have violated certain provisions of the Hatch Act, including those sections that prohibit further-restricted federal employees from taking an active part in partisan political campaigns and that prohibit any federal employee from soliciting donations or contributions for a partisan political party, candidate for partisan political office, or partisan political group.

It has come to our attention that [REDACTED] operates a twitter account under the handle [REDACTED].¹ Our preliminary review of [REDACTED] activity on the account reflects that [REDACTED] actively posts both during and outside her regular work hours. Although to the best of my knowledge, none of the tweets specifically discussed below were posted while [REDACTED] was on duty, present in a federal building, or using a federally owned or leased vehicle, OGC has not

¹ According to the information displayed in relation to the account [REDACTED] Twitter feed contains more than 165,000 posts or "tweets" and is followed by in excess of 6,200 other Twitter accounts.

Letter to OSC Hatch Unit

Page 2

had the opportunity to review every post currently available or archived on [REDACTED]'s Twitter feed to determine whether any additional tweets or re-tweets may violate the broader prohibition under the Hatch Act concerning political activity while on duty. Apparently, [REDACTED] also operates at least one additional on-line social media account, [REDACTED], which we have not reviewed in connection with this referral.

We note that [REDACTED] received Hatch Act training conducted by the Office of Special Counsel on [REDACTED] 2012. This training expressly included training concerning the prohibition against political activity through social media. As part of that training, [REDACTED] was also provided a copy of the April 4, 2012, HATCH Advisory Opinion, "Frequently Asked Questions Regarding Social Media and the Hatch Act." Attached as Exhibit F, please find a copy of the attendance roster reflecting [REDACTED] attendance, including [REDACTED] signature next to her name (see Exhibit F, page 2).

Despite the preliminary nature of our review, we have identified at minimum the following specific tweets that may constitute prohibited political activity in violation of the Hatch Act:

1. On October 17, 2012 at approximately 1:03 am EST, [REDACTED] tweeted "I just made a donation to support President Obama. TODAY IS THE FEC DEADLINE. Every dollars helps. How about you? OFA.BO/TBTmPN." The abbreviated hotlink embedded in [REDACTED]'s post currently directs the viewer to a website that appears to be a donation page related to the nonprofit organization Organizing for Action: contribute.barackobama.com/donation/orgforaction/2/index.html?source=20120706_OFA_TWS. (Attached as Exhibit A.) However, media accounts indicating that Organizing for Action was formed after the November 12 election as the successor organization of President Obama's authorized campaign committee for that election. Thus, at the time [REDACTED] posted it, the link may have directed the viewer to the Obama campaign web site. The substance of [REDACTED] comment and its timing in advance of the election also suggest this. In tweets responding to [REDACTED]'s tweet, several of [REDACTED] followers stated that they had also donated or planned to contribute to President Obama. [REDACTED]'s statement may therefore constitute a solicitation or encouragement of others to donate to a political candidate.

Letter to OSC Hatch Unit

Page 3

2. On November 7, 2012 at approximately 1:19 pm EST, in response to [REDACTED] who asked "what can I do to support the POTUS now that he's been re-elected?" [REDACTED] responded "Donate to the campaign to help pay off debt." (Exhibit B.) As such, [REDACTED] statement may constitute a solicitation or encouragement of others to donate to a political candidate's campaign committee.

3. On June 8, 2013 (Saturday), [REDACTED] stated "Yes!" in a "re-tweet" post that reads in full: "Yes! RT @CoryBooker: It's official. I'm running for Senate. Please join my campaign today: cards.twitter.com/cards/9eu4d/6a." The handle @CoryBooker is the verified twitter account for Cory Booker, then Mayor of Newark, NJ, who was announcing his intention to run for a seat in the United States Senate in the Special Election in New Jersey. Booker subsequently won the special election contest on October 16, 2013. Clicking the link included in [REDACTED] message generates a pop-up message from the Booker campaign that permits the viewer to share name and email address information with Cory Booker's campaign. (Exhibit C.) Consequently, [REDACTED] comment and re-tweeting of a partisan candidate's announcement and campaign link may constitute active participation in partisan political campaigning under the OSC guidance on social media activity, prohibited for further-restricted federal employees.

4. On September 26, 2013, [REDACTED] retweeted two comments soliciting donations for the political campaigns of Wendy Davis. Specifically, at approximately 8:30 pm EST, [REDACTED] retweeted a message sent from @WendyDavisTexas, the verified twitter account of Wendy Davis, a Texas state senator. At the time, Wendy Davis was preparing to announce on October 3, 2013, her intention to run for Governor of Texas in the 2014 election. The tweet stated "A week from today, I'm announcing something big. Can you chip in now to show the strength of our grassroots network? bit.ly/19k4lck." The abbreviated hyperlink "bit.ly/19k4lck" directs the viewer to a webpage titled "Wendy Davis for Senate | Contribute today!" (Exhibit D). The linked page solicited contributions for Davis's Texas State Senate campaign account. Thus, [REDACTED] retweeted a partisan candidate's tweet, which may constitute active participation; moreover, because the original message was a solicitation, to the extent retweeting constitutes a solicitation by [REDACTED] it may also be prohibited activity under the Hatch Act.

5. Also on September 26, 2013, at approximately 7:25 pm EST, [REDACTED] retweeted a post from the account of [REDACTED] which stated "Want to turn Texas Blue? Donate to @bgtx and @WendyDavisTexas". [REDACTED] appears to be the Twitter handle of an individual. [REDACTED]'s post retweets a solicitation to donate to @WendyDavisTexas and @bgtx. The handle @bgtx relates to the Twitter account of Battleground Texas, which is registered with the FEC as an independent political committee which, according to media accounts, seeks to promote the Democratic Party and Democratic candidates in Texas. As discussed above, @WendyDavisTexas is the twitter handle of Wendy Davis's verified twitter account. [REDACTED] therefore appears to have retweeted a solicitation to a political candidate and/or partisan political group. (Exhibit E.)

In addition to these five particular public statements on social media that may constitute violations of the Hatch Act, [REDACTED] appears to have engaged in substantial partisan political commentary on other occasions in relation to political parties and federal candidates, some of which may possibly violate the Hatch Act prohibition on engaging in "political activity" during

Letter to OSC Hatch Unit

Page 4

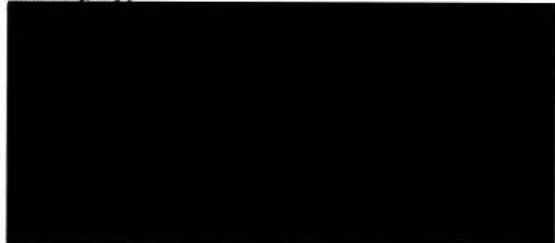
work hours (See generally Exhibit H.) In addition to commenting on the Davis and Booker campaigns, many of [REDACTED]'s older tweets relate to the presidential election contest in 2012 between then-candidates Mitt Romney and Barack Obama. Our preliminary review further suggests that often, but not always [REDACTED] would identify her Twitter commentary concerning the candidates involved in that election with the hashtag [REDACTED]" which may be accessed through Twitter's on-line search capabilities. Although we have not sought to verify whether any of [REDACTED]'s political commentary was posted during duty hours, the substantial volume of [REDACTED] activity in relation to these contests and [REDACTED] practice of regularly posting during work hours suggests that it is possible some number of those partisan political statements may have been posted during [REDACTED] regular work hours as a federal employee.

Contact information for [REDACTED] as well that of her ultimate supervisor, [REDACTED] [REDACTED] Associate General Counsel [REDACTED] is set forth below.



Should you require any further information from OGC, please do not hesitate to contact me at (202) 694-[REDACTED] or the Agency's deputy ethics official, [REDACTED] at (202) 694-1342. Thank you for your attention to this matter.

Sincerely,



Attachments

cc: [REDACTED] Deputy Ethics Official

Letter to OSC Hatch Unit
Page 5

[REDACTED]
Exhibit List

Exhibit	Document Description
A	Tweet about donating to Obama for America, with link to webpage
B	Tweet answering @xanada101's question helping President Obama after re-election
C	Retweet from Cory Booker's account announcing he's running for Senate with link to pop-up
D	Retweet from Wendy Davis soliciting donations with link to webpage.
E	Retweet from [REDACTED]
F	Hatch Act training attendance sheet dated [REDACTED], 2012
G	Pdf of tweets available as of September 27, 2013
H	Pdf of additional politically themed tweets

Attachment No. 2

Hatch Act Training Rosters
2010 and 2012

Case Number INV-13-04

Attachment No. 3

Screen capture of [REDACTED] participation in the webcast
on September 21, 2012

Case Number INV-13-04

Windows Internet Explorer

http://live.huffingtonpost.com/#r/archive/segment/512c2d7278c90a16c000f49

File Edit View Favorites Tools Help

Convert Select

Outlook - canthurber@hott... Find Result - 5 USCA § 1103 #r/archive/segment/512...

Got an iPhone? Got an iPad? We've got an app. **Download it for free!**

Like 53k Follow +1

Cadillac

H Log in

HUFFPOST LIVE

BROWSE

Earlier Nelly LIVE

Military Channel's 'Capturing Oswald'

Ken Burns LIVE

Ann Romney to Mitt Critics - 'Stop It'

Sarah Palin And Matt Lauer Have An Inane Conversation

NBC Poll: Christie Trails Clinton In Hypothetical '16 Race

Activists Say RoboRoach App Is Animal Cruelty

Bill Nye The Science Makes Awesome Surprise Visit To

WATCH FULL SEGMENT (9/21/2012)

share tweet +1 embed email

Log in Having Trouble? User Agreement Privacy Comment Policy About Us About Our Ads Send Feedback

Copyright © 2012 TheHuffingtonPost.com, Inc. "The Huffington Post" is a registered trademark of TheHuffingtonPost.com, Inc. All rights reserved. Part of HuffPost News • HPMG News

Done, but with errors on page.

Internet | Protected Mode: On 100%

Start Re: "Confidential: OIG R..." #r/archive/segment... 1:19 PM

FOIA 2016-32_370

Redactions pursuant to FOIA Exemptions 3, 6, 7(C) & 7(D)

Attachment No. 4



WebTA record and computer training room reservation
dated September 21, 2012

Case Number INV-13-04



Invitation: Emeetings with WebCam (Training Room reservation for [REDACTED])

Fri 09/21/2012 11:00 AM - 1:00

PM

Attendance is **required** for [REDACTED]

Chair: [REDACTED]

Location: 506C

[REDACTED] has invited [REDACTED] to a meeting. You have not yet responded.

Required: [REDACTED]

[Empty response area]

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.