FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

Inspection of the Federal Election Commission's Contract Security Guard Program

AUGUST 2012

ASSIGNMENT No. OIG-11-03

OFFICE OF INSPECTOR GENERAL

TABLE OF CONTENTS

GOALS, OBJECTIVES, SCOPE AND METHODOLOGY

Background

The Federal Election Commission (FEC) building at 999 E Street, Northwest, Washington, District of Columbia (the "Building"), is leased by the General Services Administration (GSA) from a private owner. The Building and FEC employees, visitors and contractors receive protection from private armed security guards, or Protective Security Officers (PSOs), under a contract (the "Contract") between the Department of Homeland Security (DHS) Federal Protective Service (FPS) and Masters Security, Inc. (Contractor).

Goals

The goals of this Office of Inspector General (OIG) inspection were twofold:

1) To review the Contract and related policies, procedures, and orders to clarify responsibilities and authorities. This goal is informational and intended to provide FEC management with an understanding of the responsibilities and authorities of the parties to and beneficiaries of the Contract. Such an understanding is crucial both in day-to-day operations and during emergencies.

2) To determine compliance and suggest policy and procedure enhancements. This goal is operational and intended to ensure compliance with selected Contract provisions, policies and procedures, and to report the results to FEC management and FPS representatives. Suggestions for enhancements in policies and procedures that are not compliance related will be offered.

Objectives

1) Identify the parties to and terms of the Contract;
2) Determine the entities that have personnel, administrative and operational responsibilities and authority concerning the PSOs, the Contract and the Contractor;
3) Identify the responsibilities and authority of the PSOs, and their chain-of-command;
4) Inspect PSO facilities, including weapons storage facilities;
5) Determine whether relevant policies and procedures, including firearms procedures, are being followed; and
6) Identify and suggest enhancements related to policies and procedures.

Scope

The inspection encompassed a review of: the Contract and associated documents; relevant policies, procedures, and orders; types of routine and incident logs, forms and reports filled out or filed by the PSOs; PSO training; duties, responsibilities and authority of the PSOs; lines of authority and communication, and chain-of-command; and the roles and responsibilities of FEC offices and personnel and non-FEC entities related to the Contract.

The inspection did not entail a technical review of the Contract, policies and procedures to determine if they are adequate, appropriate and meet federal, legal and industry standards. Further, the inspection did not include a comprehensive review of the Building's physical security, but instead was limited to those aspects of building security as they pertain to the goals and objectives of the inspection. However, any obvious deficiencies in these areas were noted and communicated to FEC management, and future inspections may address these areas.

The OIG recognizes its limits in making a recommendation and suggestions to another federal agency, in this case the FPS. Still, the OIG believes the information will be constructive in assisting the FPS in addressing the issues brought forth in this report.

Methodology

The OIG conducted the following inspection steps:

- Obtained and reviewed the Contract and associated documents, and relevant policies, procedures and orders;
- Obtained and reviewed relevant documents concerning PSO training;
- Obtained and reviewed relevant documents concerning the duties, responsibilities and authority of the PSOs;
- Obtained and reviewed relevant documents concerning the lines of authority and communication, and chain-of-command of the PSOs;
- Obtained and reviewed relevant documents concerning the administrative and operational roles and responsibilities of FEC and non-FEC entities and personnel;
- Interviewed relevant persons; and
- Inspected PSO facilities, including weapons storage facilities.

DISCUSSION

The FEC is not a party to the Contract, but rather a beneficiary of the Contract. Therefore, the FEC has a limited role in oversight of the Contract. Despite the FEC's limited oversight role, the Inspector General Act of 1978, as amended, provides authority for the FEC Office of Inspector General (OIG) to conduct audits (including inspections) of the Contract and Contract-related activities as they affect the programs and operations of the FEC. Because the Contract provides for the security of the FEC building and personnel, including the identification and screening of all persons entering the Building, it directly relates to and impacts the FEC's programs and operations.

The Contracting Officer (CO) and Contracting Officer Representative (COR, formerly referred to as the Contracting Officer Technical Representative, or COTR) are FPS employees, and the FPS is responsible for enforcement of and ensuring Contractor compliance with the Contract's provisions. Only one FEC employee is designated as an Agency Technical Representative (ATR), who has been delegated certain limited roles and responsibilities by FPS and reports directly to the COR.

The Contract was executed between FPS and the Contractor on July 28, 2010, for a performance period of October 1, 2010, through September 30, 2015. The indefinite delivery/indefinite quantity Contract covers three (3) federally leased facilities, two buildings housing the Federal Trade Commission (FTC) and one housing the FEC, in Washington, District of Columbia. The original cost for protection of the Building, the only FEC facility, was set at $31,722 per month, with provisions for Temporary Additional Services as needed. According to the COR, the fiscal year 2012 cost is $435,781, or $36,315 per month, when wage adjustments are accounted for. The COR stated a monthly invoice is generated from DHS to the FEC, funds are then transferred from the FEC to DHS, and DHS then pays the Contractor. As a non-party beneficiary of the Contract, the FEC's role is largely limited to providing funds for DHS to pay the Contractor and to receiving the benefit of the Contractor's services.

PSO Authorities and Duties

FPS has statutory authority to protect property owned or leased by the federal government, and to protect persons on and near the property, including the power to carry firearms and make arrests. 40 U.S.C. § 1315(b)(1), (2). PSOs are delegated authority by FPS to protect federal property, identify and screen employees and visitors, detain visitors creating a disturbance, and carry firearms under the terms of the Contract and its attachments, as well as the PDBs (Post Desk Books). Each of the three (3) PSO posts is issued a PDB, which is the governing document for each post and contains post orders (Guard Post Assignment Record Form 2580), bulletins, memoranda, and other documents related to the duties of the PSO at that post.

The PSOs' primary duty is "to protect lives and government property." PDB 1, at 1. According to the COR, while PSOs have contractual authority to detain visitors and employees for alleged violations of law and regulation, they do not have the authority to arrest. If a PSO detains an individual, the PSO must contact FPS immediately, or as soon as practicable, so that FPS may dispatch a sworn federal law enforcement officer. Other than screening persons and items entering the Building, PSOs have no authority to perform a search, but they may conduct limited officer safety pat-downs.

PSOs check the identities of employees and visitors entering the Building and prevent unauthorized entry. Visitors must pass through a magnetometer and their personal property is screened by an x-ray machine in an effort to detect potential dangerous or illegal items and keep them from entering the Building. Upon successful completion of this screening, the PSOs will then issue a visitor a pass and release the visitor to their employee escort. PSOs also screen items delivered to the Building through the loading dock or the lobby. PSOs are required to divert from their normal duties to respond to emergencies or incidents, including fire alarms, bomb threats, medical emergencies, and employee disturbances.

PSOs must report incidents and emergencies to FPS, although in some cases minor non-emergency incidents may be reported to the Agency Technical Representative.

Oversight and Supervision

Federal officials with authority under the Contract consist of the CO, COR and ATR. The CO and COR are FPS employees. The CO has authority to enter into, administer and terminate the Contract. The CO also makes Contract-related determinations and findings. The COR acts under a written delegation of authority by the CO and is responsible for day-

to-day administration and technical monitoring of the Contract. FPS supervision of the PSOs is accomplished administratively through the COR and operationally through the FPS Inspector assigned to the Building; both the COR and Inspector are armed, sworn federal law enforcement officers. The COR has the authority to make written modifications to the post orders so long as there is no change to the cost and the modifications do not require an amendment to the Contract itself.

A tenant agency ATR, who must be designated in writing by the FPS, acts as an extension of the COR in performing on-site Contract monitoring. For example, in an emergency, the ATR may redirect PSOs from their posts for up to four (4) hours. An ATR also provides Contractor/PSO guidance on a day-to-day basis, reports deficiencies to the Contractor and COR, and may request modifications to the post orders. There is only one FEC employee delegated authority by FPS as an ATR, and no other FEC employee has any authority under the Contract. The ATR, a supply technician in the Administrative Services Division, has held the position for over seventeen years. The ATR's training consisted of a one-week initial training session and he attends annual one-day training sessions. The FEC Administrative Division Manager is listed in some documents as the agency's Security Officer, but is not an authorized ATR according to the COR. Although the Federal Emergency Management Agency occupies one floor of the Building and is also a beneficiary of the Contract, it does not have an on-site ATR. According to the COR, only the lead agency in a leased building, in this case the FEC, has an on-site ATR.

There are no on-site PSO supervisors located at the Building.[1] The Contractor supervisor for the FEC PSOs is located at the FTC facility at 601 New Jersey Avenue, Northwest, Washington, District of Columbia.

The Contractor is required to perform a monthly quality control inspection and notify FPS of the results. Each month, FPS conducts an administrative audit of the Contract, and the COR receives updates of the PSOs' qualifications and certifications on the seventh of each month. The FPS Inspector assigned to the Building usually inspects the PSOs at least twice a week, according to the ATR. The ATR has limited authority to conduct inspections, and usually conducts a safety inspection of the security office, which is a locked secure room in the Building for PSO use, every one to two weeks; the primary focus of this inspection is to ensure firearms and ammunition are not left unsecured.

[1]This information, from the FPS COR, is contrary to that provided by the FEC ATR. While an FEC PSO displays what appear to be sergeant's chevrons on his collar, according to the COR, they are an internal Contractor designation for a lead PSO but do not designate that lead PSO as a supervisor. The FEC ATR, however, maintains that the chevrons designate that PSO as a supervisor.

Administrative Concerns

Apart from the Contract and its attachments, the day-to-day activities of a PSO are governed by several FPS-issued documents, including the PDBs, the Security Guard Information Manual (SGIM), the Protective Security Force Service Requirements (Statement of Work as attached to the Contract), and a compilation titled Commissioners and Denied Access.

PSOs are required to fill out daily forms and logs, including visitor logs. The Contract Security Guard Duty Register (Form 139) lists the names and on- and off-duty times of each PSO, the Chronological Log (Form 1103) provides a running list of daily activities, the Offense and Incident Report (Form 3155) is filled out as required for certain events like emergencies and incidents, and the Firearm and Equipment Register (Form 1051) is filled out when firearms are checked in or out. According to the COR, visitor logs are routed to the Administrative Division for review, and then they are picked up by the COR on a weekly basis and kept in the COR office. The other forms, including the Form 1051s, are sent over to the PSO supervisor's office at the FTC approximately every six to seven months, but sometimes there are delays in sending them over. The ATR also routinely reviews the forms on a monthly basis. Until the forms are forwarded, they are kept in a locked cabinet. Copies of the forms are also sometimes kept on-site in a secured area for internal purposes by the Contractor.

Title 41, Code of Federal Regulations, Part 102-74, Subpart C governs conduct on owned or leased federal property, including the authority to inspect items and identify and register visitors entering or leaving federal property. A copy of these regulations must be posted at each public entrance to federally owned or leased property.

Weapons, Use of Force and Training

PSOs assigned to the Building are armed with Contractor-provided lethal and intermediate (less-than-lethal) weapons, including semiautomatic pistols and expandable batons, as well as handcuffs. According to the COR, there are no FPS guidelines covering PSO use of force or handcuffing, and a PSO may use whatever level of force he or she believes to be necessary based on training. New PSOs have to go through FPS-mandated training and pass initial and periodic written and performance tests, including: the operation of all screening machines to which they are assigned; forty (40) hours of initial firearms training and at least semi-annual qualification; initial and annual intermediate weapon qualification; first aid, cardiopulmonary resuscitation and the use of automatic external defibrillators. PSOs must obtain and maintain all applicable licenses and certifications.

PSOs keep their firearms and ammunition stored in a Contractor-provided gun safe

A clearing barrel[2] is located next to the gun safe to facilitate the safe loading and unloading of the firearms.

[2] A clearing barrel is essentially a ballistic metal tube that one positions the muzzle of a firearm in when loading and unloading. If a round is discharged during the loading or unloading process utilizing a clearing barrel, the round should enter and be stopped in the clearing barrel where it cannot injure a person or property.

INSPECTION FINDING AND RECOMMENDATION

Finding #1

PSOs were observed using cellular telephones and other personal electronic devices while on duty and on post, most recently on February 15, 2012, at 5:30 p.m. Other violations were observed before and during the inspection by other OIG staff. Section IV of the PDBs (On Post Conduct) states that the use of cell phones is "strictly prohibited." Another section of the PDBs, a memorandum titled Special Order – Personal Conduct on Post, paragraph b, dated August 6, 1990, also bans the use of personal electronic devices. Prior to the OIG's issuance of this draft report, this issue had been addressed by FEC management. A memorandum was issued by FEC management in March 2012 to the PSOs, and meetings were held with the PSOs, PSO supervisors and FPS in May 2012.

Recommendation

The ATR, COR or Contractor should monitor the PSOs regarding the policy on the use of cellular telephones and personal electronic devices while on post; and consider possible disciplinary action if future violations occur of the policy.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

FEC Management Response:
In a memo from the Administrative Services Division Manager dated March 21, 2012 and entitled "Cell Phones on Post" the PSOs were reminded of the policy regarding the use of cellular telephones and personal electronic devices while on post. This policy was further stressed to all PSOs during the Security Update meetings held by the ASD Manager and ATR on May 17th, 18th, and 23rd. (Six security guards attended the meetings; management provided their names in the response, but OIG has removed the names from the final report.)

The ATR performs random spot-checks and limited visual monitoring of the guards, and can give verbal warning and/or report to guard's supervisor and/or FPS if a violation is noted, however, FEC does not have the authority to take any disciplinary action if future violations to the policy occur.

This finding is not very clear in terms of each party's roles and responsibilities. The ATR, COR, and Contractor each has defined roles and responsibilities. The ATR

cannot act as the supervisor and exercise disciplinary actions. However, he or she can notify the COR and the guards' supervisor, as he did when the incident occurred. It would be helpful if OIG can distinguish between ATR, COR, and Contractor's roles and responsibilities in its recommendation. FEC Management requests this recommendation be revised to clarify each party's responsibility.

OIG Comment:
The OIG agrees that FEC management took appropriate action concerning this issue, and notes that action was taken before the OIG formally notified management of the problem. Concerning the finding not being clear in terms of each party's roles and responsibilities, the OIG understands that the ATR can only make notifications to the COR and Contractor and would not expect the ATR to act outside of the appropriate parameters. The COR and Contractor should be responsible for taking disciplinary or other appropriate action pursuant to the Contract and related policies.

INSPECTION OBSERVATIONS AND SUGGESTIONS

A. FPS Policies, Procedures and Guidance

Observation #1

The Post Desk Books contain some outdated, modified or superseded information, some of which impact inherently dangerous activities such as firearms handling. The PDBs also contained expired law enforcement notices. The PDBs were provided to OIG through the ATR are dated March 9, 2009, which is prior to the commencement of the current Contract. During his interview, the COR stated that he would furnish the OIG with updated PDBs, which would include updated post orders and modifications; the FPS never provided updated PDBs despite repeated requests. Further, according to the ATR, the PDBs provided to the OIG at the beginning of the inspection were the most recent and, as of February 14, 2012, are still in effect and issued to the PSOs.

Outdated, modified or superseded policies and procedures include:

- The firearms handling procedures bulletin (Handling of Weapons at Armed Guard Posts) is dated Summer 1990 and details transfer and receiving procedures for revolvers, not the semiautomatic handguns currently used by PSOs. Some of these procedures are inherently different and inapplicable to the handling of semiautomatic pistols. There are no detailed procedures listed for the safe transfer and receiving of semiautomatic pistols.
- This procedure is currently not being followed. The COR stated that this procedure had been modified to the current practice of Despite repeated requests, FPS did not provide a copy of the written modification of this procedure.
- The PDBs contains outdated emergency contact personnel. PDB 1 has a duplicate page five (5), one of which is current and the other is outdated and lists personnel no longer with the agency, including the FEC security officer, or no longer an ATR. PDB 2 contains the same outdated page five as PDB 1. PDB 3 also contains this outdated page, but has one of the former employee's names scratched out next to the date "3/16/11." PDBs 2 and 3 do not have the current page.

- Some procedures are decades old with no indication if they have been reviewed or are still in effect. The security alert guidelines are dated September 14, 1988. Even if these guidelines are still in effect post September 11, 2001, there is nothing to demonstrate they have been reviewed in almost twenty-two (22) years or that they remain in effect without changes. There are several documents concerning found property that appear to have been superseded. A document titled "Chapter 26 Lost and Found Property Procedures" is dated September 14, 1988, but there are two older, different documents that also concern found property, a "Record of Property Found and Attempts to Contact Owner" and "Found Property Tag," both with an effective date of January 1977. The 1988 document appears to consolidate somewhat the earlier documents, but there is no indication of which procedures are in effect, other than the dates.
- Examples of federal identification cards and credentials appear to be outdated. For instance, the samples of FPS credentials indicate they are issued by GSA (of which FPS was previously a component), not DHS.
- The Protective Security Force Service Requirements (Statement of Work) requires that PSOs carry certain certifications, including current weapons and first aid cards, on their person when on duty. The COR stated that these requirements had been modified and that the certifications were now kept on file by the Contractor, but there is no written record of these modifications in the PDB or elsewhere. According to the ATR, the ATR receives a monthly report from FPS detailing the PSOs' certifications status (weapons, first aid).

Suggestion

FPS should review and update the PDBs, including the post orders and firearms handling procedures. FPS should solicit suggestions from the ATR and the FEC Security Officer in this process. Expired notices and outdated information should be purged. Older policies and procedures still in effect should include dated documentation that they were reviewed and remain in effect without changes or revisions. Updated PDBs should be distributed to all PSOs, the ATR and the FEC Security Officer. All applicable modifications to the post orders of Protective Security Force Service Requirements (Statement of Work) should be documented in each PDB.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

Observation #2

There are no guidelines concerning use of force by PSOs assigned to the FEC. According to the COR, the use of deadly force, including the drawing and use of firearms, and less-than-lethal force is totally within the PSO's discretion. Even if PSOs are trained in using a use of force matrix or to follow a use of force policy, it appears that once a PSO has completed training and is on post, the PSO is not required to follow any FPS use of force policy.

Likewise, according to the COR, there is no written policy covering the use of handcuffs,

Suggestion

FPS should develop and implement a written use of force policy for PSOs assigned to the FEC, to include deadly and less-than-lethal force. A policy covering the use of handcuffs should also be developed and implemented. The Department of Justice Policy Statement on Use of Deadly Force (1995) and the example of a use of force continuum on the Department of Justice's National Institute of Justice website could possibly be adopted for PSOs.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

B. FEC Communication

Observation #3

FEC has not recently communicated to staff information about PSO duties and authorities, and how to report problems. For instance, over the past two years, the OIG has occasionally received reports of alleged deficiencies concerning PSOs assigned to the Building, instead of the reports being made directly to the ATR. While it may be good practice to keep the OIG informed of deficiencies, complaints must be properly routed to the ATR to ensure deficiencies are addressed by the proper parties.

Suggestion

The ATR or FEC Security Officer should send an email to all FEC employees and contractors detailing the proper procedure for reporting complaints and alleged deficiencies concerning PSOs. This email should be sent at least annually, and these procedures should be included in the New Employee Orientation and posted on the FEC intranet.

FEC Management Response:
FEC management can develop procedures for reporting complaints and alleged deficiencies concerning PSOs. This information can be included in the New Employee Orientation packet that ASD provides and posted on the ASD FecNet page (currently under construction).

OIG Comments:
The OIG agrees with the FEC management response.

Observation #4

The FEC does not have enough designated ATRs. In the event the current ATR is on leave or out of the Building, there is no one to take over his duties. While it is advisable to have an alternate ATR available to handle routine issues in the ATR's absence, it is critical in an emergency. In calendar year 2011 alone, there were two emergencies that affected the Building – an earthquake and smoke from an overheated HVAC unit – demonstrating the need for alternate ATRs.

Suggestion

FEC management should collaborate with FPS to officially designate and train at least two alternate ATRs. The Administrative Division Manager should be considered for this position. A chain-of-command and communication plan between the ATRs should be developed to prevent confusion in case a PSO receives conflicting orders from two ATRs during an emergency.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

FEC Management Response:
It is recommended that the ASD Manager be one of the alternate ATRs. The

Occupant Emergency Coordinator, also a member of the ASD staff, is recommended as the 2nd alternate, as this individual usually serves as Acting in the absence of the ASD Manager. FEC will contact FPS to determine what steps are required to officially request and assign alternate ATRs.

OIG Comment:
The OIG agrees with the FEC management response.

C. PSO Practices

Observation #5

Firearms records are not filled out properly. During the physical inspection of the security-related facilities and records on January 19, 2012, the OIG found that all Forms 1051 were improperly filled out in that boxes 1-8 were left blank. These boxes, not all of which are individually numbered, contain general "header" information, such as "unit" and "building." This discrepancy was confirmed with the COR, who was present during the inspection.

Suggestion:

The COR should report this practice to the Contractor and ensure retraining of all PSOs on how to properly fill out the Form 1051.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

D. Additional Suggestions

Observation #6

The Commissioners and Denied Access book contains information and photographs of persons denied access to the Building, including some former employees. It is important for PSOs to have photographs of banned persons, in addition to their names and descriptions, in order to quickly be able to identify potentially dangerous persons, including former FEC employees who may pose a threat to other FEC employees. In some instances, notices revoking building access for former FEC employees were placed in the book without a photograph of the former employee. New FEC employees and contractors whose contract

term is for at least six (6) months have their photographs taken for Personal Identity Verification (PIV) cards, but the FEC cannot print copies of PIV cards or the photographs on PIV cards. The FEC "generally" also photographs new employees for the Intranet directory. During the OIG's exit meeting with FEC management for this inspection, FEC management advised the agency does comply with the Homeland Security Presidential Directive (HSPD) 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*. In addition, FEC management agreed to research the capabilities available that could further strengthen the information provided to the PSOs on current employees and contractors.

Suggestion

FEC management should ensure that each new employee and contractor is photographed, and should maintain that photograph on file in the event it is ever needed for identification purposes or to be placed in the List of Commissioners and Banned Persons. FEC management should also ensure it has identification photographs of each current FEC employee and contractor.

FEC Management Response:
FEC management will ensure photos are taken of employees during the new employee orientation on-boarding process. In regards to contractors and unpaid interns, FEC management will explore options for this suggestion including taking their photo when they report to Human Resources for the fingerprint process or HSPD12/PIV registration. In some instances, especially for external person(s), short-term visitors, etc., a photograph will not be available for all banned persons.

OIG Comment:
The OIG agrees with the FEC management response.

Observation #7

The Rules and Regulations Governing Conduct on Federal Property is posted at the Building's public entrance pursuant to 41 C.F.R. 102-74.365, and is located on the side of the x-ray machine and next to the magnetometer facing the public. The document is on approximately letter-sized paper. While arguably technically compliant, if a visitor does not have any items to be screened in the x-ray machine and does not look toward the x-ray machine when passing through the magnetometer, the document may be easily overlooked and, in any event, is difficult to read unless one is in close proximity. This could lead to a potential legal defense of inadequate notice if a visitor or employee is charged with a violation.

Suggestion

FEC management should produce a larger, poster-sized version of the Rules and Regulations Governing Conduct on Federal Property, and place it in a more prominent location so that it is clearly visible to everyone entering the Building, including visitors, contractors and employees.

FEC Management Response:

FEC management will explore options for this suggestion. Most other federal agencies do not have a "poster-sized" version of these rules and regulations; however, we will look into making the document larger and more visible for individuals entering the building. We have also included this document in the New Employee Orientation packets that ASD provides to new employees.

OIG Comment:

The OIG agrees with the FEC management response.

Observation #8

There are two instances where there is no policy or procedure to notify the OIG of security-related issues over which the OIG may have jurisdiction or an interest. Currently, the OIG is not notified when a person is placed on the list of persons banned from access to the Building. However, any time a person is banned from the Building for cause, especially a terminated employee or contractor, it is possible the OIG may have jurisdiction over the actions that led to the individual being banned. Further, a banned person may also be a witness or subject of an OIG investigation, and therefore it would be critical for the OIG to be informed if the witness or subject has been banned from the Building.

The OIG is also not routinely notified of security incidents involving the Building or FEC employees, contractors or visitors. However, it is probable that any security incident would at least technically fall under the jurisdiction of the OIG.

Suggestion

FEC management should adopt a policy of notifying the OIG whenever a person is placed on the list of persons banned from access to the Building. Additionally, the COR should issue a written modification to the post orders so that the OIG is notified of any security incident. A notification will not necessarily lead to OIG action, especially if the incident is one of concurrent jurisdiction more appropriately handled

by another agency, but the OIG should at least be made aware of all security incidents.

FEC Management Response:
The ASD is operationally in charge of the agency's security, in conjunction with DHS/FPS policy and procedures. Due to the confidential and sensitive nature of some security situations, the parameters of this request on the types of information bi-laterally shared will be determined on a case-by-case basis. FEC management is agreeable with providing the OIG copies of security memos related to current or former FEC employees, when applicable.

OIG Comment:
It is the statutory duty and responsibility of the OIG to conduct and supervise audits and investigations relating to the programs and operations of the agency, including security incidents as they relate to FEC operations. *See* 5 U.S.C. App. 3 §§ 2(1), 4(a). The OIG is entitled to have access to all records, reports and other material relating to the OIG's statutory duties. *Id*. at § 6(a). Further, section (b)(1) of the Privacy Act of 1974 allows for intra-agency disclosures of information when necessary in the performance of duty. Therefore, the OIG has concurrent jurisdiction with other FEC components and law enforcement agencies concerning security incidents that relate to FEC operations or programs, and the OIG is legally entitled to all information necessary to perform its duties regarding security incidents, not just on a case-by-case basis.

Importantly, the OIG often conducts investigations, the details of which are not known to FEC management. A security incident may occur involving a complainant, witness or subject of an OIG investigation, or the person may be terminated or placed on the denied access list, either of which may have a direct bearing on the OIG investigation. If FEC management is unaware of the OIG investigation or its details, the incident or denied access listing may not be reported to the OIG, resulting in the OIG taking a course of action that it otherwise would not have had it been informed of the security incident. Potentially, FEC management's failure to inform the OIG of a security incident or denied access listing could compromise a criminal, civil or administrative investigation.

For the reasons that the OIG is legally entitled to reports of all security incidents related to FEC programs or operations that fall within the OIG's investigative jurisdiction and that failure to report a security incident could jeopardize an investigation, the OIG disagrees with FEC management's response that it will only provide information on a case-by-case basis or when applicable. Rather, the OIG

should be promptly informed of all security incidents and on every occasion when a person is placed on the list of banned persons.

Observation #9

According to the ATR, when a PSO separates or is terminated from the Contractor's employment, there is no requirement that the electronic combination to the Contractor-provided gun safe be changed. While a former PSO would likely not be allowed entry to the Building and security office, it is still possible for this to happen, which would then provide the former PSO with access to a deadly weapon and ammunition stored in the gun safe. If a former PSO were to obtain a Contractor-issued firearm and ammunition in this manner, it would present a danger to FEC employees, visitors, contractors, current PSOs and the general public.

Suggestion

FPS should modify the post orders to require a change in the combination of the gun safe any time a PSO separates or is terminated from employment by the Contractor.

FPS Response:
FPS was provided a copy of the draft report on August 6, 2012, but did not furnish a response by the due date of August 22, 2012.

CONCLUSION

The OIG's goals to review the Contract, policies and procedures, standing orders, and guard facilities to clarify responsibilities and authorities, and to determine compliance with selected Contract provisions, policies and procedures, and suggest policy and procedure enhancements were met during this inspection. While none of the observations or the finding poses an immediate risk to FEC programs or operations, and do not indicate fraud, waste or abuse, the observations concerning firearms and use of force guidelines potentially pose a liability risk to the government and should be addressed as priorities. The other observations and finding should also be promptly addressed in order to provide clarity of duties and roles, and improve communication and the efficiency and effectiveness of the contract security officer program.

The inspection did not cover the legal and technical aspects of the Contract and the Building's physical security. FPS has primary legal and contractual oversight authority concerning the Contract and PSOs. While the FEC's role is limited, communication between the ATR, FPS and the PSOs is critical to ensuring that established policies and procedures are followed in fulfilling the mission of protecting persons and FEC property.

LIST OF ACRONYMS

ATR	Agency Technical Representative (FEC employee)
CO	Contracting Officer (FPS employee)
COR	Contracting Officer's Representative (FPS employee)
DHS	Department of Homeland Security
FEC	Federal Election Commission
FPS	Federal Protective Service
FTC	Federal Trade Commission
OIG	Office of Inspector General
PDB	Post Desk Book (contains orders and procedures for each post)
PSO	Protective Service Officer (security guard)

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.