

**Office of Inspector General  
Inspection of the Agency's  
Checkout Process  
OR09-01**



**January 2009**

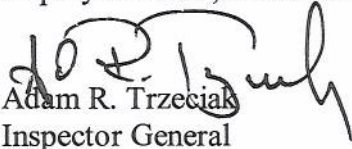


**FEDERAL MARITIME COMMISSION**  
Washington, DC 20573-0001

January 12, 2009

*Office of Inspector General*

**TO:** Anthony Haywood  
Deputy Director, Office of Administration

**FROM:**   
Adam R. Trzeciak  
Inspector General

**SUBJECT:** Inspection of the Agency's Checkout Process

The Office of Inspector General completed a program inspection of the agency's checkout process for separating employees. The objective was to assess whether controls are in place to remove separated employees from agency systems and databases, to collect outstanding balances, and to retrieve agency materials and equipment. As employees are provided charge cards, travel and transit subsidy advances, personal data assistants and access to the FMC network containing sensitive data, both practical and security-related considerations dictate that the agency diligently control the return of agency-provided property and access to its information systems.

***Background***

Commission Order (CO) 54, *Clearance of Employee Accountability*, dated December 3, 2004, provides guidance to agency managers and separating employees regarding the checkout process. The order states, in part, that *all government-issued property will be returned to the issuing office in good condition before the employee is granted final FMC clearance. Failure to adhere to this policy may result in the withholding of final check(s) due the employee.* A record is maintained on Form FMC-25, *Employee Clearance Statement* a checklist for separating staff used to confirm that all agency-supplied equipment and materials have been returned.

The *Employee Clearance Statement* is a critical component of the check out process as it holds both the departing employee and program office staff accountable. It requires the separating employee to certify, in writing, that all government property and records have been

returned and all debts settled. For its part, program/office staff clearing the separating employee must ensure that claims made by the separating employee are accurate and that all agency-owned material is returned. The FMC offices and functions identified on the checkout form are: the employee's program office; Office of Management Services (OMS); Office of Human Resources (OHR) with the function of the Information Security Officer (ISO); Office of Financial Management (OFM); Office of Information Technology (OIT); the Librarian; and the Ethics Officer. The completed form is then submitted to OHR for final clearance and is filed in the employee's payroll file. The following roles and responsibilities are associated with each clearance station:

**Employing office** performs an annual/sick leave audit, ensures records, bound volumes and security classification documents are returned. The employing office also is responsible for returning contractor badges to OHR.

**Office of Management Services** collects unused transit benefits and office keys. OMS also notifies the FMC's administrative service-provider, the Bureau of Public Debt (BPD), to revoke purchase (charge) cards (if applicable) and access to the procurement and financial system (if granted), and the Department of Transportation to terminate employee participation in the transit subsidy program (if applicable).

**Office of Human Resources** collects employee identification (ID)/access cards and performs exit interviews (non-mandatory). Both employee and contractor IDs are shredded and access cards returned to OMS for reprogramming. OHR also provides final clearance of the employee, ensuring that all required signatures were obtained by the separating employee.

The **Information Security Officer** performs security clearance debriefings of separating employees.

**Office of Financial Management** collects travel (charge) cards and notifies BPD to revoke card privileges in the on-line travel system and confirms that the employee has no other debt to the agency. OFM also collects agency-issued passports (when applicable) for return to the State Department.

**Office of Information Technology** revokes access to agency information systems and collects personal data assistants from staff. OIT requires departing employees to provide barcodes from their personal computers, monitors and other agency-issued devices, such as Blackberries and printers. Employees are also required to provide OIT with voicemail password and telephone calling cards (if issued). The information collected is used by OIT to update its inventory and to remove the employee's computer equipment from his/her work station.

The **Librarian** verifies that separating employees have returned borrowed library materials and revokes employee access to Westlaw.

The **Ethics Officer**, in the Office of the General Counsel, verifies that the separating employee has submitted annual financial disclosure statements (if required) and provides post-employment counseling (i.e., “do’s and don’ts”).

### ***Objectives, Scope and Methodology***

The objectives of this program inspection<sup>1</sup> were to assess whether the agency has implemented controls to (i) remove separated employees’ access from service provider systems and agency databases, (ii) collect outstanding balances, and (iii) retrieve agency materials and equipment.

The OIG reviewed CO 54, *Clearance of Employee Accountability*, to become familiar with agency guidelines pertaining to employee separations; CO 80, *Security*, to identify the responsibilities of the Information Security Officer pertaining to employee separations; and CO 91 *Employee/Visitor Identification Program*, to document the process used by the agency to cancel employee badges.

We interviewed staff in the OMS, OHR, OFM, and OIT, as well as the Ethics Officer and the Librarian to document their respective responsibilities, processes and systems each uses to checkout separating employees. We identified all employees that left the agency between October 1, 2006, and May 30, 2008 - a total of 29 employees and one student-volunteer (unpaid) - to test the agency’s checkout procedures. In the offices identified below, we performed the following inspection activities:

**Office of Management Services:** The OIG performed tests to determine if employees were revoked from agency systems (procurement and financial) and government programs (transit benefits and purchase cards) timely. We compared employee separation dates with (i) revocation dates for select agency systems, and (ii) purchase card, transit benefit and access card cancellation dates.

We reviewed the timing and content of correspondence sent by agency staff to BPD to cancel separating employees’ purchase cards. We reviewed purchase card statements and supporting documents to determine whether purchases occurred after the employees’ separation. We compared notifications sent by OMS staff to the Department of Transportation (DOT) to cancel employee transit benefits with DOT reports identifying employee-benefit cancellation dates to determine whether employees were removed timely. We also reviewed access card (i.e., key card) vendor reports to verify that all separating employees had building access privileges revoked on their separation date.

---

<sup>1</sup> An “inspection” includes evaluations, inquiries, and similar types of reviews that do not constitute an audit or investigation. An inspection evaluates programs and activities for the purpose of providing information to managers for decision making; making recommendations for improvements to programs, policies, or procedures; and identifying where administrative action may be necessary.

**Office of Human Resources:** We reviewed checkout forms for employees (CO 54 does not provide guidance for contractors and student-volunteers) separating during the period of our review to determine whether (i) all employees provided a check out form to OHR and (ii) the employees obtained clearances from all offices identified on the form. We also checked whether all employees were granted final FMC clearance and identified actions taken by OHR against separating employees who lacked one or more certifying signatures.

**Office of Financial Management:** The OIG tested the timeliness of notifications OFM sent to BPD to revoke employee access to the on-line travel portal (GovTrip) and to cancel travel cards. We reviewed steps taken by the agency to return official United States Government passports to the State Department to assess the timeliness of these activities.

**Office of Information Technology:** The OIG tested OIT processes for revoking network access from separated employees.

**Library:** We compared employee separation dates to Westlaw access termination dates. We also obtained Westlaw-usage logs from September 2007, through February 2008, to verify that staff did not continue to access Westlaw after separating from the agency.

We did not review agency actions to collect outstanding balances. The OIG did identify one instance where an employee separated with a balance owed, but the amount was small (\$13.50) and this debt was owed to the employee's travel card.

We performed this inspection in conformance with *Quality Standards for Inspections* from July 2008 through October 2008.

### ***Inspection Findings***

#### **1. Key card Access Cards are Generally Controlled for Separating Employees**

Commission Order 54, *Clearance of Employee Accountability* dated December 3, 2004, requires, among other things, that separating employees return government property in their possession to the appropriate offices and to reimburse the agency for any outstanding balances owed. Officials, for their part, are required to certify that property is accounted for. To enforce this requirement, the Director, OHR, has the authority to withhold the employee's final paycheck.

The Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* requires that access to resources and records be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained.

Agency employees, contractors and student-volunteers are provided ID cards to gain building access. Guards located in the building lobby check each ID before permitting access to the elevators. However, due to the numerous tenants in the building – including non-federal tenants, it is difficult for the guards to become familiar with the myriad of ID logos and formats used by staff entering the building.

As an added measure of security, the agency provides “key cards” to staff, which must be scanned at one of the eight card readers located at entrances to agency offices. The mechanical readers do not distinguish card holders; any valid card will gain entry to agency office space. Therefore, it is critical that the agency closely control who is assigned an access card. The agency should maintain an updated list of all card holders and their respective card numbers. This ensures that only authorized employees maintain a key card.

While the agency does not maintain a control listing of ID card holders, OMS maintains a list of current key card holders through the card vendor’s database. Only OMS staff has access to the key card database to activate and deactivate cards. As part of our review, the OIG obtained the vendor’s list of card holders for review. As of October 1, 2008, there were a total of 165 (active) key cards issued to employees, contractors and other non-FMC employees. The OIG took a closer look at FMC employees and contractors, and other federal-agency tenants, to assess the effectiveness of the agency’s checkout / card cancellation procedures.

**TABLE 1. ACTIVE KEY CARDS AS OF OCTOBER 1, 2008**

<b>Access Card Holders</b>	<b>Number of Cards Issued</b>
FMC Employees	128
FMC Contractors	5
Other Federal Agency	12
Building Management	8
Cleaning Staff	9
Security Guards	3
	<b>165</b>

The vendor’s access card report identifies the name and card number for each card holder. For the agency to maintain the integrity of the listing, it must update the list when employees separate from the agency. The OIG found that the agency is generally doing a good job deactivating former agency employees from the key card list. However, it needs to coordinate better with the Social Security Administration (SSA), a co-tenant on the 10<sup>th</sup> floor headquarters building, to control custody of the cards.<sup>2</sup>

The OIG’s review of the active card list identified nine key cards that were assigned to former building employees. Seven of the cards were assigned to SSA staff, one card was

<sup>2</sup> The SSA/OIG maintains a field office for its agents on the 10<sup>th</sup> floor of the FMC’s headquarters building.

assigned to a former FMC employee and one card was assigned to another federal employee temporarily assisting an FMC program office.

Of the seven cards assigned to SSA, three cards are reassigned to new employees not in the FMC access card database and three cards are unassigned. One card is missing. The SSA did not notify the agency regarding the assignment changes or lost card, and the FMC has not proactively contacted the SSA to check the status of the cards assigned years earlier. Consequently the active card user list maintained by the FMC is inaccurate. Should the three unassigned cards become lost or stolen, they could be used to gain access to FMC office space. The lost card should be deactivated immediately.

An access card and ID assigned to another federal employee temporarily working with an FMC program office was returned to OHR in November, 2006. OMS has custody of the card but has not deactivated it. Should this card become lost or stolen, it could be used to gain access to FMC office space.

The OIG also identified a student-volunteer that left the agency without returning his ID or key card. The student-volunteer was employed from May – August, 2006, and was provided an identification badge, access card, transit benefits and access to the agency's Network. When separating, this employee did not check out and did not return agency property that was provided to him.

Student-volunteers present special challenges because they are not required to check out when separating, putting the responsibility on the student-volunteer's supervisor to collect all agency materials and revoke access to agency systems through OIT. The OIG notes that many students today possess substantial technical skills that they can use to exploit agency controls designed to prevent system abuse. It is especially important to revoke access to all agency systems by separating students to limit the agency's exposure to possible cyber abuse or attack.

The student-volunteer's program office made multiple calls to him regarding outstanding agency property. After several months, the student-volunteer informed staff (in November, 2006) that he lost both the identification badge and access card. The OIG verified that the lost card was deactivated by our October, 2008, fieldwork dates. (The key card system does not record cancellation dates, so we could not determine when the card was deactivated.) The agency was potentially at risk during the period the key card (and I.D.) was not controlled by the agency.<sup>3</sup>

---

<sup>3</sup> Although outside the review scope; the OIG identified six duplicate cards issued to FMC staff and one duplicate card issued to a building custodial worker. With two exceptions, the employee reported the original card lost, and a new card was issued. But the lost card was not deactivated by the end of our fieldwork. Until the card is returned and/or deactivated, the agency is vulnerable to unauthorized access.

## 2. Clearance Signatures Missing on Some Employee Clearance Forms

The Form FMC-25, *Employee Clearance Statement* is used to hold separating employees and managers accountable for agency property and the security of agency information. The completed form, by the eight previously-identified agency “clearance stations,” is submitted to OHR for final certification. To ensure compliance by separating staff, the CO authorizes OHR to withhold all or a portion of the separating-employee’s final paycheck if the employee has outstanding balances due or unaccounted-for equipment.

We reviewed the *Employee Clearance Statements* for 29 employees (one student-volunteer was not required to submit a clearance statement) to ensure that clearances were obtained before separating from the agency. We found that all separating employees provided OHR with the checkout form. However, seven employees did not obtain clearance (signatures) from all required clearance stations identified on the form. Three of the seven employee forms were missing two certifying signatures while the remaining four employee forms lacked one signature. The missed clearance stations are identified below:

**TABLE 2. MISSING CERTIFICATIONS BY CHECKOUT STATION FOR SEVEN EMPLOYEES**

Offices	Employing Office	OMS	ISO	Library	OHR	Ethics Officer	OFM	OIT	Total
Occurrences	3	0	1	1	4	0	0	1	10

The OIG could not determine why select signature lines were not signed. In all instances, OHR staff provided final certification for the seven employees, in effect, approving the separation. There was no indication on the forms that OHR had contacted the missing clearance officials to obtain a verbal certification or that OHR had sought to withhold the employee’s final paycheck. Without such signatures, the agency has no assurances that the seven employees returned all agency-owned property or had access revoked from agency information systems.

In a related test, we reviewed the checkout forms to determine whether separating employees provided barcodes (as required) from their personal computer, monitor and other OIT equipment. This is the only section on the checkout form that requires the employee to provide information on government-issued property. The OIG identified six (of 29) separating employees that did not provide barcode information for FMC equipment. We also noted that all six employees were cleared by OIT staff. OIT management stated that, as a general rule, OIT staff enters the barcodes on the form when separating employees do not.



### 3. Clearance Form Omits Select Commission Services

Agency employees use a number of information systems to perform their job responsibilities. These systems include the FMC Network, PRISM, Discoverer, GovTrip, Westlaw, and the System for Time and Attendance Reporting (STAR).

The Network permits employees to access e-mail, Internet and other systems that are housed on the Network's infrastructure. PRISM, Discoverer, GovTrip, STAR-NFC and Westlaw are automated services that provide various support functions, including procurement, budget, accounting, travel and payroll information. Westlaw is an on-line legal research library that assists with all phases of the litigation process.

The checkout form identifies systems that all employees are generally provided access to but does not identify select systems / databases only some employees can access. When an employee goes through the checkout process, the agency relies upon the certifying official to inquire of the separating employees as to which systems they have access to. The form does not assist management in the checkout process by including all agency systems or services, thereby potentially leaving systems or benefits susceptible to being missed. Any valid (i.e., open) account on agency systems and databases poses some risk to the security of the system. It is best to eliminate those risks when former employees are involved.

### 4. Employees are not removed from Systems Timely

We found that even when separating employees were cleared by the eight respective clearance stations on the *Employee Clearance Statement*, employee access to systems e.g., e-mail, Westlaw, PRISM, etc., or benefits, e.g., travel card and transit benefits, was not always timely revoked. The GAO *Standards for Internal Control in the Federal Government* requires that access to resources and records be limited to authorized individuals only. Separated employees are not authorized users of service provider systems and agency benefits.

#### *Purchase and Travel Card*

Employees are provided purchase and/or travel cards to perform their duties for the agency. There were two of 29 separating employees provided purchase cards and 24 of 29 separating employees provided travel cards (including access to GovTrip). To obtain these cards and access to the travel system the employee must submit a request to the program coordinators in OMS and OFM, respectively.

The program coordinators in OMS (purchase card) and OFM (travel card and GovTrip travel service) submit a request to BPD for issuance of the government credit cards and travel service access for employees. These managers are also responsible for providing BPD with written notification to cancel a separating employee's purchase and travel card and GovTrip access. BPD cannot cancel an employee's card or access to the system until the request is made.

The OIG reviewed OMS and OFM requests to BPD to cancel cards. In both instances, the OIG identified delayed notifications to BPD which prevented their being timely removed from these respective systems. For the two employees assigned purchase cards, OMS did not notify BPD for two and four weeks respectively, after the employees separated. Management stated these delays were attributed to charges made on the purchase card up to the separation date.

Management told the OIG that not deactivating cards for several weeks provides little risk to the agency because the cards are collected (although not always cancelled) when the employee separates from the agency. However, the OIG notes that card numbers are used for all on-line transactions, and an unscrupulous employee could simply copy the card number before returning the card.

Due to the risk purchase cards present (purchase card charges are billed directly to and paid by the agency), these cancellation requests should be made on the employee's separation date.<sup>4</sup> Once BPD learned of the employees' separation, it reduced the purchase card holder's account limit to \$1.00. If either employee had gone to another BPD-customer agency, that employee would not have been able to obtain a purchase card because FMC did not timely cancel these accounts. Both employees were cleared by the Director, OMS.

Twenty-four (24) of 29 employees that left the agency had travel cards and/or access to GovTrip assigned to them. We reviewed OFM requests to BPD to deactivate these travel cards and revoke GovTrip access. When an employee separates from the agency, an OFM staff notifies BPD through e-mail. BPD acknowledges the request and provides notification when action(s) have been taken via an email. This email also informs FMC that the travel card will be cancelled within two weeks after the effective date of departure to allow for any pending documents to process through the system.

For five (5) of the 24 employees with travel cards and access to GovTrip, the OIG found that the agency required between 39 days and 257 days to request card deactivation from BPD.<sup>5</sup> In the latter example, the agency only became aware that the employee's account was not closed when the travel card was reissued. Management informed us that notification was sent to BPD in October 2007 to cancel the employee's travel card and access to GovTrip. Management was not sure why the card was reissued.

We verified through BPD that the card was not used after the employees' separation date. Management correctly noted that since the agreement is between the cardholder and the card company, the agency is not at financial risks. The following table illustrates the number of days that lapsed between the employee's separation date and OFM notification to BPD.

---

4 The OIG verified with the card vendor that neither employee used the purchase card after separating from the agency.

5 The actual days lapsing before OFM notified BPD to cancel card and travel system privileges for five employees were: 39 days, 39 days, 53 days, 81 days and 257 days.

**TABLE 3. LAPSED DAYS BETWEEN EMPLOYEE SEPARATION AND OFM NOTIFICATION TO BPD**

<b>Number of Days Lapsed</b>	<b>Number of Employees Issued Travel Cards</b>
Less than 14 days	17
15 – 30 days	2
30 days or more	5
Total	24

OFM told the OIG that it reduces employee card limits to \$20 when employees are not in travel status. Most likely, this limit was in effect for the eight employees whose accounts remained open 15 – 257 days after leaving the agency. (The OIG did not verify these limits.) However, with employees leaving the FMC for jobs at other federal agencies, it is imperative that access to these systems and use of travel cards be timely suspended, as these former employees would not be able to obtain a new travel card with a different agency while the FMC travel card is still active. We are aware of one instance where a former employee could not obtain a GovTrip account because her profile was still active with FMC. Management explained that the agency was paying for a local voucher that had not completed the process cycle when the employee separated. OFM notified BPD of this employee’s separation 14 days after she left.

***Agency Issued Passports***

Select senior managers are provided official U.S. Government passports for use when traveling abroad on agency business. The OIG identified two employees with passports. Both employees returned the passports to the agency prior to separating (in November 2006 and February 2008). Both passports were returned to the State Department for cancellation in February 2008.

***PRISM/Discoverer***

*PRISM* is an online procurement system that facilitates the paperless processing of requisitions and purchases. *Discoverer* is an online reporting tool that allows real time access to an organization’s financial data.

The OIG identified nine (9) of 29 separating employees with access to one or both of the systems (PRISM/Discoverer). When an employee leaves the agency OMS staff sends an email to BPD or uses BPD’s *Administrative Resource Center Online Applications Access Request Form*, to remove the employee from the system. We spoke to BPD to obtain the dates when the nine employees were removed from PRISM and/or Discoverer. We compared the date the employee left the agency with the system revocation date. One employee’s access to PRISM was still active six months after leaving the Commission. During our inspection, OMS sent notice to BPD to cancel this employee’s access in mid-October 2008. OMS sent the formal notification to cancel the other eight separated employees in March/April 2008.

### *Transit Benefits*

Metro checks are transit subsidies provided to eligible Federal employees to reduce their commuting expenses to and from work on public transportation. To receive benefits, employees submit an *Application for Transit Benefits* to their immediate supervisor for approval. The form is then forwarded to the Directors of Administration and Office of Management Services for their approval before the transit benefits are disseminated to the employee. An OMS staff member is the coordinator for this program and provides the DOT with employee information needed to add him/her to the agency's benefit roster.

When employees separate from the agency, they must satisfy all outstanding transit benefit liabilities (i.e., those benefits paid in advance but unused as of the employee's separation date). Outstanding balances are repaid by the return of unused metrochecks or by a personal check. The program coordinator notifies DOT that an employee has left the agency. The agency receives a quarterly report from DOT identifying all benefit recipients for the preceding quarter which should be used by the coordinator to check for errors or unauthorized use.

There were 21 of 30 separated employees that participated in the transit program. (The student-volunteer is considered an employee for purposes of the transit benefit program.) Eight of these 21 employees had withdrawn from the program months/years prior to leaving the agency. Of the remaining 13 separating employees, six remained on the eligible benefit rolls for 30 days or more after leaving the agency. The following table illustrates lapsed days between the employee's separation and the request to terminate benefit participation (to DOT):

**TABLE 4. LAPSED DAYS BETWEEN EMPLOYEE SEPARATION AND DOT NOTIFICATION**

Lapsed Days	Number of Employees
Less than 14 days	3
15 – 30 days	4
30 days or more <sup>6</sup>	6
Total	13

By not withdrawing the employee from the transit benefit program timely, separating employees could continue to download their monthly benefits, unless the program coordinator routinely checked DOT's quarterly participation report. Even with this routine check of the quarterly report, an employee could receive three months of unauthorized benefits before the error is detected.

---

<sup>6</sup> The actual days lapsing before OMS notified DOT regarding transit benefit cancellations were: 48 days, 79 days, 102 days, 122 days, 136 days and 136 days.

### *Westlaw and FMC Network*

Westlaw is an online legal research service that allows individuals to access research libraries and practice tools for all phases of legal and non-legal research. The FMC procures these services for both its legal and non-legal staff. The Librarian is responsible for providing access to Westlaw and canceling that access when an employee leaves the agency. Westlaw Rapid Password Manager is used by the Librarian to set up or cancel an employee's access to Westlaw. At the time an account is set up for an employee, the ID/password is emailed to the named individual. Once the Westlaw-issued 'ID/password card' is received by the Librarian, it is delivered to the employee.

The librarian is also responsible for clearing separated employees against borrowed books/periodicals that may have been checked out under their names.

The OIG reviewed employee access and usage records for the period of September 2007 through February 2008. During this period, the OIG identified 10 employees who had been given access to Westlaw in furtherance of their work for the FMC, and who had subsequently left the FMC. We found that access to Westlaw was generally revoked 14 days or less from the date the employee departed the agency. However, during this review period we found that Westlaw accounts that had been set-up for 2 employees who subsequently left the agency, had not been cancelled until 2 and 4 months after their separation, respectively. Our review of Westlaw research logs for the period previously identified found that neither of these employees used the services after they left the FMC.

The agency's network allows employees to have access to internal systems. OIT staff is responsible for revoking Network access for separating employees. OIT makes a copy of the checkout form for its files and the employee's access is removed from the Network at the end of the "last workday."

We sent a "test" e-mail through Outlook to determine whether all 30 employees that left the agency were removed from the network. We identified 2 accounts that remained open as of July, 2008, months after the employees' separation dates. (The two employees departed the agency in April and May, 2008.) One of the accounts responded with an out of office auto reply.

The OIT management informed us that even though these accounts "appear" to exist, the account credentials cannot be used to access any part of the FMC Network. Further these email accounts remained open by the request of the employing office supervisor for business purposes. These emails are monitored by staff and are filtered.

### *Inspection Recommendations*

To address the findings presented above, the OIG makes the following eight recommendations for corrective action to the Deputy Director of Administration:

#### Recommendations Pertaining to Finding 1:

1. Request staffing information from SSA biannually to update the authorized list of key cards.
2. Maintain custody of unassigned cards or, at a minimum, deactivate cards that are in the custody of SSA but not assigned.
3. Immediately deactivate the lost SSA card.
4. Update Commission Order 54 to include checkout procedures for contractors, student-volunteer and other Federal agency staff assigned key cards.

#### Recommendations Pertaining to Finding 2:

5. Instruct the Office of Human Resources to contact clearance stations when their certifying signatures are missing on the checkout form and annotate the record with details of the contact (date, person spoken to, clearance provided).
6. Amend CO 54, *Employee Clearance Statement*, to include payroll-related sanctions (i.e., withholding of final paycheck) as a reminder to separating employees to obtain all certifications on the checkout form.

#### Recommendation Pertaining to Finding 3:

7. Amend FMC-25, *Employee Clearance Statement*, to include the universe of systems and benefits that employees have access to, including Westlaw, Discoverer, PRISM, STAR, and GovTrip, to assist certifiers when revoking system access.

#### Recommendation Pertaining to Finding 4:

8. Amend FMC-25, *Employee Clearance Statement*, to require access to all agency systems be revoked within one day of the employee's separation.

**\*\*\* MANAGEMENT COMMENTS \*\*\***

# FEDERAL MARITIME COMMISSION

## Office of Administration

### Memorandum

**To :** Inspector General

**Date:** January 2, 2009

**From :** Deputy Director of Administration

**Subject :** Comments on Draft Inspection Report on the Agency's Clearance Process

I have reviewed the recommendations in the instant Inspection. Below are our comments regarding corrective actions which will be effected to address the recommendations.

#### Recommendations pertaining to finding #1.

1. Request staffing information from SSA biannually to update the authorized list of key cards.
2. Maintain custody of unassigned cards or, at a minimum, deactivate cards that are in the custody of SSA but not assigned.
3. Immediately deactivate the lost SSA card.
4. Update Commission Order 54 to include check-out procedures for contractors, student-volunteer and other-Federal agency staff assigned key cards.

**Response.** OA agrees with points 1, 2 and 3 of finding #1. The list of authorized key cards assigned to SSA staff should be updated biannually. The SSA-assigned key card reported as lost was deactivated by OMS. By March 31, 2009, OMS will develop an SOP for key cards. As part of the development of this SOP, OMS will consider how to improve custody and control of key cards issued to FMC employees, SSA and/or other federal agency staff needing access to FMC space. As to point 4, C.O. 54 and Form FMC-25 will be reviewed for possible revision by June 30, 2009.

#### Recommendations pertaining to finding #2.

5. Instruct the Office of Human Resources to contact clearance stations when their certifying signatures are missing on the checkout form and annotate the record with details of the contact (date, person spoken to, clearance provided).



6. Amend Form FMC-25, *Employee Clearance Statement*, to include payroll-related sanctions (i.e., withholding of final paycheck) as a reminder to separating employees to obtain all certifications on the checkout form.

**Response.** OA agrees with both points 5 and 6 of finding #2. The Form FMC-25, *Employee Clearance Statement*, should have all necessary certifying signatures when employees leave the agency. Effective immediately, OHR will require that Forms FMC-25 submitted by departing employees are complete, and will not accept incomplete forms. Regarding point 6, OA notes that the instructions for the form currently state that "Clearance of employee accountability as evidenced by completion of this form must be on record in the FMC's cross-servicing agent's Payroll Office before release of final salary check...." By June 30, 2009, OA will develop an SOP regarding the agency's clearance process and will revise Form FMC-25 to clarify this language.

**Recommendation pertaining to finding #3.**

7. Amend Form FMC-25, *Employee Clearance Statement*, to include the universe of systems and benefits that employees have access to, including Westlaw, Discoverer, PRISM, STAR, and GovTrip, to assist certifiers when revoking system access.

**Response.** OA agrees that access to the universe of systems and benefits to which employees have access should be revoked as soon as possible after their departure. The SOP to be developed by OA by June 30, 2009 regarding the agency's clearance process will address systems access termination and may include language requiring the employing office to identify the systems to which a departing employee has access. OA will evaluate the necessity of amending Form FMC-25. Further, OA will look into the possibility of automating this form by September 30, 2009 and will provide a status report by June 30, 2009 on this effort.

**Recommendation pertaining to finding #4.**

8. Amend FMC-25, *Employee Clearance Statement*, to require access to all agency systems be revoked within one day of the employee's separation.

**Response.** OA agrees that departing employees' access to all agency systems should be revoked as soon as is practicable, either prior to separation or as soon as possible after separation. By June 30, 2009, OA will develop an SOP regarding the agency's clearance process and will review C.O. 54 and Form FMC-25 for possible revision.

If you have any questions about these comments, please let me know.

  
Anthony Haywood