NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

REVIEW OF FACILITY SECURITY
AT
NCUA'S CENTRAL OFFICE

Report #OIG-11-06
June 23, 2011

William DeSarno
Inspector General

Released By:

James Hagen
Deputy Inspector General

Auditor-in-Charge:

Charles E. Funderburk, CPA
Senior Auditor

CONTENTS

ACRONYMS AND ABBREVIATIONS

CCTV	Closed Circuit Television
COOP	Continuity of Operations
DHS	Department of Homeland Security
DO	Designated Official
DOJ	Department of Justice
FCA	Farm Credit Administration
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
FOUO	For Official Use Only
FPS	Federal Protective Service
FSC	Facility Security Committee
FSL	Facility Security Level
ID	Identification
IDS	Intrusion Detection System
ISC	Interagency Security Committee
NCUA	National Credit Union Administration
OIG	Office of Inspector General
PSI	Protection Strategies Incorporation
SBA	Small Business Administration
SEC	Security and Exchange Commission
SSP	Senior Staff Position

Preface

Protecting Federal employees and the public who visit U.S. government owned- or leased-facilities is a complex and challenging responsibility. From the terrorist attacks of September 11, 2001, and the subsequent Brentwood Postal Facility anthrax case that same year, to the more recent hostage situation at the Discovery Channel building in Silver Spring, Maryland, as well as the recent incidents involving the ignition of incendiary devices in packages that were mailed to two state office buildings in Maryland, the need to provide heightened protection for Federal facilities and those who occupy and visit them has never been more critical. In light of these more recent attacks, the NCUA Board rightfully requested the Office of Inspector General (OIG) move up its timetable for performing its 2011 planned review of building security measures at the NCUA's Central Office and Region II facility.

In the broad and constantly evolving area of security and, in particular, physical security at Federal facilities, we in the OIG do not hold ourselves out as experts in the field. However, we approached this review in the same objective manner we conduct all of our reviews and believe we have developed a report that will not only help the NCUA Board and management make decisions today that will help close the gap on several security vulnerabilities we detected, but will also provide a roadmap to plan for vulnerabilities that the agency might face in the future.

This report outlines current Federal guidance and NCUA's adherence to this guidance, provides the OIG's assessment of NCUA's current physical security measures in place, and makes three recommendations the OIG believes are crucial to helping ensure NCUA's facility and its occupants continue to remain safe.

Executive Summary

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted a review of facility security at NCUA's Central Office. We reviewed facility security to: (1) assess the adequacy of physical building security measures at NCUA's Central Office. Within this objective, we placed a particular emphasis upon reviewing building security access and controls, specifically related to: (a) security operations and administration; (b) facility entrance security; (c) security systems, and (d) site and interior security. To achieve these objectives, we interviewed management and staff in NCUA's Division of Procurement and Facilities Management (DPFM); conducted physical observations of current building security controls and operations; reviewed NCUA policies and procedures related to building security; benchmarked with five Federal agencies, and obtained and reviewed Department of Homeland Security's (DHS) security facility risk assessment standards.

We determined NCUA's current security environment is not adequate. Specifically, we found physical security deficiencies in non-compliance with Interagency Security Committee (ISC) standards, as well as specific facility risk vulnerabilities that expose the facility to greater risk of undesirable events. As a result, we are making three recommendations to correct these deficiencies. Management agreed with our first recommendation and agreed with all but one aspect of our second recommendation. However, management disagreed with our third recommendation. The OIG considers all three recommendations as resolved. [redacted]

We appreciate the cooperation and courtesies NCUA management and staff provided to us during this review.

Background

In 1993, the NCUA purchased the building located at 1775 Duke Street in Alexandria, Virginia as office space for its Central Office and Region II staff. Currently, the NCUA has approximately 250 employees working in this office location. The NCUA office building (facility) is part of a larger office complex, which includes three other office buildings and a hotel, as well as a shared underground parking garage. The facility has seven floors and approximately 167,000 square feet of usable space. There are four tenants within the facility. NCUA is the primary building tenant occupying most of the first floor and all of floors 2 through 7. The other three tenants--an investment firm, an education center and a retail shop--occupy space on the first floor with each having separate entrances for pedestrian traffic. Neither of these tenants has space directly connected to or accessible to NCUA occupied space.

The facility is located in an overall commercial section of Alexandria, primarily populated with office buildings and some retail establishments. Nearby is a major rail station, a Federal courthouse, and the U.S. Patent and Trademark Office complex.

Physical Security Guidance

Federal, as well as NCUA's, physical security standards have evolved over time. In 1995, the U.S. Department of Justice (DOJ) established the first set of Government-wide physical security standards for Federal facilities. After the Oklahoma City bombing of the Alfred Murrah Federal Building in 1995, the President ordered a vulnerability assessment of all Federal facilities to terrorism or violence. The DOJ issued a Vulnerability Report, which developed minimum physical security standards for civilian federally owned or leased facilities.

In January 1996, the NCUA issued Instruction No. 1063 to establish security processing procedures for employees and contractors in the Central Office. In December 1996, NCUA management rescinded Instruction No. 1063 and issued Instruction 1063.1, which established agency procedures on building access control for the facility. The revised instruction essentially implemented a security program utilizing identification (ID) badges for all employees as well as detailed instructions for visitors.

[redacted]

- [redacted]

[redacted]

- [redacted]

This latest ISC standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. This includes existing buildings, new construction or major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities, Federal campuses, and where appropriate, individual facilities on Federal campuses; and special-use facilities. Accordingly, the NCUA is subject to the ISC standards.

In September 2010, NCUA management issued a safety and security reminder to all Central Office and Region II staff covering a variety of security related issues. The memo reminded staff to ensure photo IDs are worn and visible at all times while in the facility; set forth instructions for processing visitors (e.g. pre-register, magnetometer, and escorting at all times), and cautioned staff to not allow unauthorized individuals to enter the building by means of "piggybacking."[3]

[redacted]

[2] This interim standard has a 24-month comment period before final issuance.

[3] For purposes of this report, the term "piggyback" refers to allowing someone to gain access into a facility either with another person or behind another person that does not display an appropriate picture ID.

Physical Security Assessment

Although the Department of Homeland Security's Federal Protective Service (FPS) performs building security reviews as part of its mission, we determined FPS only performs these services for GSA owned and/or leased properties and does not venture beyond those parameters. Accordingly, NCUA contracted with Protection Strategies Incorporated (PSI), a private security support firm,[4] for a physical security assessment of the NCUA facility. In October 2010, PSI completed its assessment of NCUA's physical security program and issued its report to the NCUA. PSI assessed the NCUA facility in seven major categories, [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

Despite PSI's rather comprehensive review of NCUA's physical security measures currently in place, as well as its recommendations to correct the identified deficiencies, we believe the review stopped short in addressing one very basic and important, physical security concern – [redacted]

The OIG's 2011 Annual Audit Plan included a review of security measures at the NCUA's Central Office and Region II facility. The NCUA Board, upon review of the OIG's Annual Audit Plan, requested that the OIG accelerate the timetable for this review and asked that it be conducted immediately.

[4] According to PSI's website, PSI provides security support services to many agencies within the Federal Government as well as private corporations nationwide and overseas.

Objectives, Scope, and Methodology

The objective of our review was to assess the adequacy of physical building security measures at NCUA's Central Office. Within this objective, we placed a particular emphasis upon reviewing building security access and controls, specifically related to: (a) security operations and administration; (b) facility entrance security; (c) security systems, and (d) site and interior security.

The scope of our review covered building security measures in place at NCUA's Central Office and Region II facility located at 1775 Duke Street in Alexandria, Virginia during the period from December 2010 to June 2011.

To accomplish our objective we:

- Interviewed management and staff in NCUA's Department of Procurement and Facilities Management (DPFM), a component division of the NCUA Office of the Chief Financial Officer;
- Conducted physical observations of current building security controls and operations;
- Reviewed NCUA policies and procedures related to building security;
- Reviewed a recently-completed risk assessment report prepared by a private contractor for DPFM;
- Reviewed NCUA's self assessed risk level;
- Benchmarked with five Federal agencies[5] to determine the extent of physical access security measures in place; and
- Obtained and reviewed DHS' security facility risk assessment standards for comparison with NCUA's facility risk assessment and overall adherence to the standards.

We conducted this review from December 2010 through June 2011 in accordance with generally accepted government auditing standards, and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

[5] The five benchmarked agencies are the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Federal Reserve), Securities and Exchange Commission (SEC), Farm Credit Administration (FCA), and the Small Business Administration (SBA). *(Note: The SBA was chosen because of similarities with their parking garage. Both SBA and NCUA allow the public to park in their garages.)*

Results in Detail

Overall, we determined NCUA's current building security program is deficient [redacted] Although we determined the facility risk assessment to be adequate, we found significant physical security deficiencies [redacted]

A. Facility Risk Assessment

NCUA's Risk Assessment Rating is Adequate

[redacted] Specifically, we found DPFM's self-assessment of security risks under the five areas of the ISC standard[6] to be reasonably assessed and adequately justified. As a result, we are confident the level of protection established by the ISC standard [redacted] facility will provide the proper degree of security over the facility and its operations, its occupants or visitors, and the mission of the agency.

As previously mentioned, ISC standards require all federal agencies perform a self-assessment of their overall building security risk against a baseline set of five equally weighted security factors[7] in order to arrive at an FSL designation.

Table 1 (below) provides NCUA's self-assessed risk ratings and scores for each of the five criteria as well as the OIG's assessment of NCUA's rating decision:

[6] Homeland Security's: *Facility Security Level Determinations for Federal Facilities, An Interagency Security Committee Standard, 2008.*

[7] The FSL matrix uses five equally weighted security factors to be evaluated, with corresponding points of 1, 2, 3, or 4 (low, medium, high, very high) allocated for each factor.

Table 1

Security Criteria Area	NCUA Assessment	OIG Assessment	Points
[redacted]	[redacted]	[redacted]	[redacted]
• [redacted] • [redacted] • [redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
• [redacted] • [redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
• [redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
• [redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
• [redacted] • [redacted]			
[redacted]			[redacted]

[redacted]

Table 2 (below) provides the FSL matrix levels by point value as well as DPFM's preliminary and final assessed FSL rating.

Table 2

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Intangible Factors		Raise Score One Level		Agree		[redacted]
[redacted]						
NCUA's Final Assessed FSL Rating						[redacted]

As noted in Table 1, the OIG agrees with each of the DPFM ratings given for each of the five FSL criteria. We also agree with DPFM's decision (Table 2) to raise the preliminary FSL rating by one level for the intangible factors listed. [redacted]

According to the ISC Standard,[10] each FSL corresponds to a level of risk, which then relates directly to a level of protection and associated set of baseline security measures. Comparatively speaking, an FSL Level I facility faces a minimum level of risk, and thus the baseline level of protection for a Level I facility is "Minimum;" Level II corresponds to Low; Level III to Medium; Level IV to High; and Level V to Very High.

Table 3 (below) describes the relationship between the FSL, risk, and the baseline level of protection:

[9] ISC Standards indicate Level V designated facilities receive "very high" score values across all five security criteria areas and are raised one level due to intangible factors. A facility can also be a Level V if it receives a "very high" score value for 'Criticality' or 'Symbolism' and is a one-of-a-kind facility (or nearly so). The decision-making authority for identifying Level V facilities are within the purview of the individual agency.
[10] *Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard*, issued April 12, 2010.

Table 3

Facility Security Level	Level of Risk	Baseline Level of Protection
[redacted]	[redacted]	[redacted]

[redacted]

B. Physical Security

Physical Security Measures Need Improvement

Physical security measures at the NCUA's Central Office facility are in need of improvement. Through inquiry and observation, we found deficiencies and vulnerabilities in NCUA's overall baseline level of protection in [redacted] ISC security criteria. As a result, not only is the agency not in compliance with ISC security standards, but the degree of physical security is undermined. [redacted]

There are numerous criteria within each physical security category (See Appendix A for a complete list), and the NCUA complies with many of these criteria. However, our report focuses on only those areas (deficiencies) we believe NCUA management either needs to be made aware, or action needs to be taken to limit the identified risks. [redacted]

Security Operations and Administration Needs Improvement

Experienced Designated Security Official and Security Committee Needed

During this review, we learned that NCUA's current designated official (DO) responsible for building security is a CU-1640-13 Facility Manager. NCUA built facility security duties into that position in 1989. Although the incumbent has

[redacted]

occupied the Facility Manager position since 1989 and gained significant on-the-job experience since then, this individual had no previous experience or specialized formal training in security, safety, and emergency management. Nevertheless, responsibility for facilities and physical management is a critical element of the DO's job description.

The DPFM Director supervises the DO. While the Director, DPFM, likewise has had no specialized formal training in facility physical security, this individual's background includes 35 years of significant experience in physical security. However, even though the DPFM Director has overall responsibility for the management of facility security at NCUA, none of the position's duties mentions security or safety responsibilities.

According to ISC Standards, every Federal department or agency should:

- Identify a DO who is responsible for security, safety, and emergency management;
- Establish an FSC to provide security, life safety, and emergency procedure oversight; and
- Provide a federal security manager with oversight responsibility for guards and other physical security operations that is on-site at least weekly.

Although NCUA technically meets the requirement of the ISC standard because the agency has identified a DO responsible for the safety and security of the facility and its occupants, we believe the position should be staffed by an expert in the field of security. We found that all of our benchmarking partners have DO's at the office or division director level with responsibility for overseeing every aspect of facility security. These DO's have specialized security backgrounds and qualify as experts in the field of security. We believe the duties and responsibilities of the DO position at NCUA should be removed from the existing Facility Manager position and a separate position should be created. The new position should require that the incumbent be qualified as a bona fide security expert in the field.

In addition, we also determined NCUA does not have an official facility security committee (FSC) to address facility-specific security and safety issues, as ISC recommends. The role of such a committee is to bring forth all security-related proposals for countermeasures before NCUA management for approval/non-approval and implementation, as necessary. Lacking an FSC, we believe, exposes the facility, its occupants, and the mission of the agency to risks.

[redacted]

[redacted]

Recommendations

We recommend NCUA management:

1. Revise the current Facility Manager (CU-1640-13) Position Description by removing all references to physical security related functions of the position.

Management Response

Management agreed with the OIG's recommendation to remove references to physical security-related functions from the position description of the Facility Manager.

OIG Comment

The OIG concurs with management's planned action.

We recommend NCUA management:

2. Create and staff one permanent full-time position to serve as the NCUA's Designated Official and/or federal security manager. The incumbent should possess physical security expertise, and will be responsible for all security related matters. Such duties and responsibilities should include (but not be limited to):

    a. Assessing facility security levels in accordance with ISC standards at all NCUA owned or leased facilities;
    b. Assessing building security vulnerabilities at all NCUA owned or leased facilities;
    c. Recommending building security measures to address facility security levels, vulnerabilities, and cost/benefit analysis;
    d. Overseeing all aspects of NCUA physical security operations;
    e. Overseeing all aspects of personnel security
    f. Overseeing all NCUA employee safety related functions;
    g. Involvement with all agency Continuity of Operations (COOP) efforts;
    h. Serving on the Facility Security Committee outlined in Recommendation 3, below.

Management Response

Management agreed with the OIG's recommendation to create and staff one permanent full-time position to serve as NCUA's Designated Official and/or federal security manager. However, with respect to 2.e. (above), management believes that personnel security duties should remain in the Office of Human Resources.

OIG Comment

The OIG concurs with management's planned action to create and staff one permanent full-time position to serve as the NCUA's Designated Official and/or federal security manager. However, the OIG does not agree with management's planned action to retain the duties of personnel security within the Office of Human Resources. The OIG believes a more efficient and effective solution would be to include all building and personnel security duties under the newly created Designated Official position. The OIG believes this would not only consolidate all security-related matters, but also ensure that the Designated Official is aware that anyone granted unfettered access to the building has been properly cleared.

We recommend NCUA management:

3. Create a Facility Security Committee in accordance with all applicable ISC standards responsible for addressing facility-related security and safety issues and presenting all security measures and practices to NCUA management for approval/non-approval and implementation, as necessary.

Management Response

Management does not agree with the establishment of a Facility Security Committee. Management believes security improvements should be raised to executive management through the existing budget approval process.

OIG Comment

The OIG defers to management's decision to consider security improvements through the annual budget request for consideration by the Office of the Executive Director and ultimately, the NCUA Board.

Facility Security and Construction Plans Needed

[redacted]

According to ISC standards, every Federal department or agency should have a written facility security plan identifying at a minimum:

- Security responsibilities;
- Current and planned security measures;
- Building specific security policies;
- Emergency contacts;
- Incident response procedures; and
- Contingency plans for temporary upgrades.

[redacted]

Because no such plan exists, NCUA's build-outs and renovations, as well as all future construction renovation projects, could pose increased facility risk.

Insufficient Security Screening

We determined [redacted] According to ISC standards for a every Federal department and agency should:

- Screen all mail and packages using x-ray at a loading dock or screening location; and
- Physically inspect items that cannot be passed through screening equipment.

[redacted]

[redacted]

Insufficient Security Training

We determined NCUA staff training on facility safety and security related matters is insufficient. We concluded this because DPFM officials do not sponsor regular security training. Although the agency provides employees with occasional safety reminders through e-mails, the most recent in September 2010, we believe DPFM needs to ensure that employees are kept up to date with regularly scheduled facility security training. By not conducting such training to raise employee and contractor safety and security awareness, we believe the current culture where employees do not appear sensitized to challenge unauthorized visitors will never change.

According to ISC standards, departments and agencies [redacted] should provide all employees with annual security awareness training. Four of the five agencies we benchmarked against provide employees with security training and safety reminders. We believe that NCUA can do more to ensure employees are aware of security risks and learn how they can better protect themselves and their co-workers.

Facility Entrance Security Needs Improvement

[redacted]

ID Badges Not Regularly Worn

We determined through observation there are still employees who do not wear or visibly display their employee identification badges, despite ISC standards and NCUA policy requiring that they wear an agency photo ID that is visible at all times when in the facility. Specifically, during the period of our review, OIG staff observed on three separate occasions that four individuals in the facility did not display an appropriate facility ID badge. In addition, we performed a controlled test where one OIG staff person circulated in the facility throughout the fieldwork phase of this review (December through February) without visibly displaying an appropriate facility ID badge.[13] Neither the security guards on duty nor any other NCUA employee

[redacted]

[13] The OIG staff person did have their employee identification badge on their person; however, it was not visible. In addition, this OIG staff person has not visibly displayed their employee ID badge when in the building for over five years, without challenge.

challenged this OIG employee.[14] When agency identification badges are not visibly displayed, the risk of unauthorized persons circulating in the building is increased.

Visitors Not Always Screened

[redacted]

No Use of X-Ray Equipment

We determined personal belongings and hand-carried packages entering the building are not subject to X-ray screening. However, personal belongings are

[14] Note: Security guards challenged the OIG employee when entering the facility through the Diagonal Road entrance during normal guard hours.
[15] Normal business hours are 8:00 a.m. to 5:00 p.m.; Monday through Friday.
[16] Each visitor arrived with overcoats and computer bags, and one carried a purse.

[redacted]

visibly and physically searched by security guards during normal business hours. [redacted]

Unauthorized Facility Entry

We determined there is a risk that unauthorized persons can gain entry into the facility during periods of time when the security guards are, and are not, on duty. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Security Guard Coverage and Visitor Registration is Insufficient

[redacted]

[redacted] By NCUA not having adequate security guard coverage, we believe facility security risk is greatly increased and question whether facility occupants would be safe if an undesirable event occurred at a time when security guards were not on duty.

In addition, although employees are required to pre-register visitors through the automated system so security staff will know who is expected for the day, on two different occasions during this review, OIG staff was unable to pre-register visitors through the agency's automated system because the system was down and unavailable. Despite this, the guard at the main guard desk telephonically notified the OIG that our non-registered visitors had arrived. The ISC standards indicate every [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Security Systems Need Improvement

Security systems need improvement. [redacted] As a result, the level of protection provided to facility occupants from the potential harm and consequences from an undesirable event is increased.

Closed Circuit Television Coverage and Monitoring Lacking

We determined NCUA's current CCTV coverage needs improvement. [redacted] Interagency Security Committee standards indicate that agencies should provide coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, and lobbies. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Duress Alarms Insufficient

We determined the number and location of duress (alarm) buttons throughout the facility is insufficient. Through observation, we noted only two alarm buttons located near the bank of elevators in the parking garage. According to ISC standards, duress buttons or call buttons should be located at guard posts and sensitive public contact areas. In addition, we found no duress buttons in or near the two guard posts in the main lobby, nor did we find duress buttons in the fire escape stairwells, an area we believe to be sensitive due to their isolation and direct access to public space. Without adequate duress (alarm) buttons, the level of facility security and protection is diminished in case of an emergency.

[redacted]

[redacted]

[redacted]

Site and Interior Security is Lacking

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

C. Conclusion

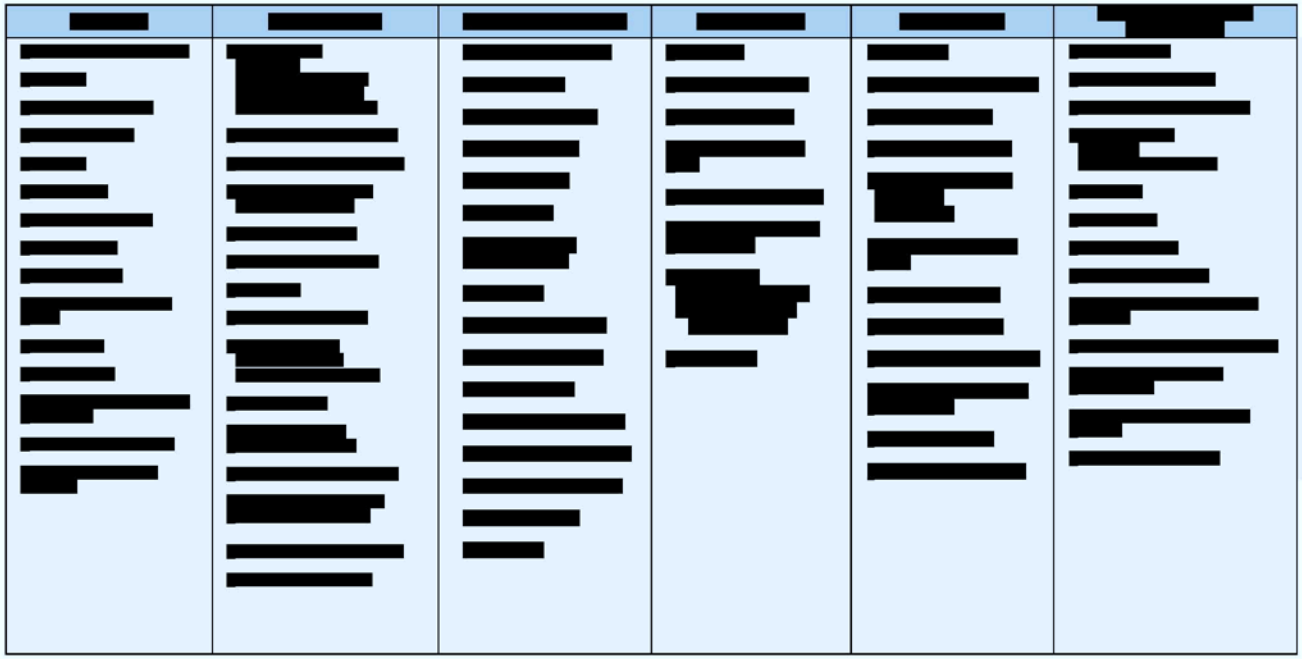
Security Vulnerabilities Need Immediate Attention

The issues discussed in this report serve to highlight the importance of a robust security program to minimize the numerous identified vulnerabilities in NCUA's overall security environment--issues we believe that require NCUA management's immediate attention, starting with the three recommendations we are making in this report.

[redacted]

status of building security at NCUA, we believe the three recommendations set forth on page 12 of this report are reasonable and well grounded. [redacted] Therefore, by leaving these decisions with the DO, we believe this individual would assist the agency in making those decisions that work best for the level of protection and the level of risk NCUA management is willing to accept to keep the facility and its occupants safe.

Appendix A: [redacted]



Appendix B: Management Response

National Credit Union Administration

TO: William Desarno
Inspector General

FROM: Mary Ann Woodson
Chief Financial Officer

SUBJ: Management Response to OIG Review of Facility Security
At NCUA's Central Office

DATE: May 24, 2011

The Office of the Chief Financial Officer (OCFO) submits the following comments in response to the Office of Inspector General's "Review of Facility Security at NCUA's Central Office," dated April 2011. Items that related to the Office of Human Resources and the Office of Chief Information Officer were coordinated with those offices.

The following comments pertain to the Results in Detail Section, beginning on page 7 of the subject report.

A. Facility Risk Assessment: (page 7)
OIG comments: NCUA's Risk Assessment Rating is [redacted]
OCFO comments: Concur with OIG comments.

B. Physical Security: (page 10)
OIG comments: Physical Security Measures Need Improvement.
OCFO comments: Comments will be provided for each section.

Security Operations and Administration Needs Improvement: (page 10)
OIG comments: Experienced Designated Security Official and Security Committee Needed.
OCFO comments: While OCFO concurs that a Designated Official responsible for building security that is experienced in the CU-0080 Physical Security career field would enhance the security program at NCUA, OCFO does not concur with the comments concerning a "lack of previous experience in security, safety, and emergency management" on behalf of the Facility Manager as being detrimental to the physical security at NCUA. The physical security program at NCUA has been successful under the oversight of the Facility Manager.

With regard to the creation of a Facility Security Committee (FSC), OCFO does not concur that a committee is necessary. Rather, security improvements should be raised to executive management via the existing budget approval process of vetting requirements/requests through DPFM management to the CFO for inclusion in the mid-year or annual budget request for consideration by the OED and ultimately, the NCUA Board.

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6300

[redacted]

Recommendations (page 12)

With respect to OIG recommendations:

1. OCFO concurs with the recommendation to remove references to physical security-related functions from the position description of the Facility Manager.
2. OCFO concurs with the recommendation to create and staff one permanent full-time position to serve as NCUA's Designated Official and/or federal security manager.
    a. With respect to recommendation 2e, OCFO recommends that personnel security duties remain in the office of Human Resources (OHR). OHR concurs that the function should remain with OHR.
    b. With respect to recommendation 2h, OCFO does not concur that a committee is necessary. Rather, security improvements should be raised to executive management via the existing budget approval process of vetting requirements/requests through DPFM management to the CFO for inclusion in the mid-year or annual budget request for consideration by the OED and ultimately, the NCUA Board.
3. OCFO disagrees with establishment of a Facility Security Committee. See comments above.

[redacted]

OIG comments: [redacted]

OCFO comments: OCFO concurs that [redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

ID Badges Not Regularly Worn (page 14)

OIG comments: [redacted]

OCFO comments: Concur. [redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: Concur. [redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

[redacted]

OCFO will seek to educate employees [redacted]

[redacted] This change in procedures has been forward to OHR/LR for presentation to the Union.

[redacted]

OIG comments: [redacted]

OCFO comments: [redacted]

[redacted]

OCFO will periodically remind offices to use [redacted]
NCUA security procedures require [redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: OIG comments are correct. [redacted]

[redacted]
with each other or DPFM facilities staff and building engineers.

OIG comments: [redacted]
OCFO comments: [redacted]

OIG comments: [redacted]
OCFO comments: [redacted]

[redacted]

[redacted]

OIG comments: [redacted]

OCFO comments: OCFO recognizes that [redacted]

Encl

Attachment 1- DPFM Security Enhancements

PHYSICAL SECURITY ENHANCEMENTS IMPLEMENTED BY DPFM

The following is a list of security improvements made to the building since NCUA moved in September 1993.

Compiled by OCFO/DPFM Facilities Management – April 2011

Attachment 1