U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Physical Security Program

August 1, 2014
Report No. 523

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

August 1, 2014

To: Jeffery Heslop, Chief Operating Officer, Office of the Chief Operating Officer

From: Carl W. Hoecker, Inspector General, Office of Inspector General

Subject: *Audit of the SEC's Physical Security Program,* Report No. 523

Attached is the Office of Inspector General's (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) physical security program. The report contains nine recommendations for corrective action that, if fully implemented, should strengthen the SEC's physical security controls.

On July 7, 2014, we provided agency management with a draft of our report for review and comment. In the July 30, 2014, response, management fully concurred with eight of our nine recommendations and partially concurred with the remaining recommendation. As a result of management's response, we revised Recommendations 6 and 8. Management's complete response is reprinted as Appendix VII in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how your office will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the review. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Mary Jo White, Chair
Erica Y. Williams, Deputy Chief of Staff, Office of the Chair
Luis A. Aguilar, Commissioner
Paul Gumagay, Counsel, Office of Commissioner Aguilar
Daniel M. Gallagher, Commissioner
Benjamin Brown, Counsel, Office of Commissioner Gallagher
Michael S. Piwowar, Commissioner
Mark Uyeda, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein

Anne K. Small, General Counsel, Office of the General Counsel
Timothy Henseler, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Barry Walters, Director/Chief FOIA Officer, Office of Support Operations
Cedric Drawhorn, Assistant Director, Chief of Security Services, Office of Support Operations
Cedric Watson, Branch Chief, Physical Security Operations, Office of Security Services, Office of Support Operations
Thomas A. Bayer, Director, Office of Information Technology
Pamela C. Dyson, Deputy Director, Office of Information Technology
Todd K. Scharf, Associate Director, Chief Information Security Officer, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Michael Whisler, Assistant Director, Office of Acquisitions
Paul Levenson, Regional Director, Boston Regional Office
Lynn Austin, Assistant Regional Director, Boston Regional Office
Andrew M. Calamari, Regional Director, New York Regional Office
Robert Keyes, Associate Regional Director, New York Regional Office
Jina L. Choi, Regional Director, San Francisco Regional Office
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Audit of the SEC's Physical Security Program
Report No. 523
August 1, 2014

Why We Did This Audit

The Government Accountability Office has designated Federal real property management as a governmentwide high-risk area due, in part, to the continued challenge of protecting Federal facilities. At the U.S. Securities and Exchange Commission (SEC), the Office of Security Services (OSS) is responsible for the physical security and safety of SEC staff and facilities at the agency's 11 regional offices, 2 data centers, and headquarters in Washington, D.C. In 2011 and 2012, the Office of Inspector General (OIG) investigated physical security violations, and recommended a review of the agency's physical security program. As a result, the OIG contracted with Ollie Green & Company, CPA's, LLC (referred to as "we" in this report) to assess the SEC's policies, procedures, and controls for safeguarding personnel and preventing unauthorized access to the agency's facilities.

What We Recommended

To provide reasonable assurance that the SEC's policies, procedures, and controls effectively safeguard personnel and prevent unauthorized access to the agency's facilities, we made nine recommendations for corrective action. The recommendations address policies and procedures; risk assessments; facility security plans; issuance of badges; access-controlled doors; contractor performance; data center controls; and training. Management concurred with eight of the recommendations and partially concurred with one recommendation. The recommendations will be closed upon completion and verification of appropriate corrective action. Because this report contains sensitive information about the SEC's physical security program, we are not releasing it publically.

What We Found

We visited the SEC's headquarters, three of its regional offices (b)(7)(F) and its two data centers, and obtained information from personnel at the remaining SEC locations. From our observations and the information we obtained, we determined that improvements are needed in the SEC's physical security controls. Specifically, we identified the following physical security vulnerabilities:

- facility risk assessments were incomplete, outdated, or not performed;
- facility security plans did not identify all current or planned security measures;
- SEC-issued badges were not always properly controlled;
- some access-controlled doors were unsecured; and
- the SEC's security system contractor monitored the agency's physical access control and intrusion detection systems from an offsite location, and did not always notify the OSS of alarm conditions.

In addition, the SEC's (b)(7)(F) lacked sufficient security measures to prevent unauthorized, undetected, and undocumented access to key information technology assets.

During the audit, management took action to address some of the conditions we observed; however, the conditions occurred because the OSS did not adequately manage and administer the SEC's physical security program. Specifically, we found that

- the OSS did not establish effective policies and procedures to address required Federal physical security standards;
- the OSS did not ensure that physical security program internal controls were measured and tested;
- security specialists' competencies did not always match their assigned roles and responsibilities; and
- the OSS outsourced security systems responsibilities to a contractor but did not provide sufficient oversight to monitor the contractor's performance.

The results of our audit indicate that action is required to establish a comprehensive physical security program and that doing so will reduce the risk to SEC personnel, facilities, and property.

For additional information, contact the Office of Inspector General at (202) 551-6061 or www.sec.gov/about/offices/inspector_general.shtml.

TABLE OF CONTENTS

ABBREVIATIONS

CCTV	closed circuit television
FOUO	For Official Use Only
FSL	facility security level
HSPD-12	Homeland Security Presidential Directive 12
ISC	Interagency Security Committee
IT	information technology
Kastle	Kastle Systems
OG&C	Ollie Green & Company, CPA's, LLC
OI	Office of Investigations
OIG	Office of Inspector General
OIT	Office of Information Technology
OSO	Office of Support Operations

OSS	Office of Security Services
SEC	U.S. Securities and Exchange Commission
U//FOUO	Unclassified//For Official Use Only

Background and Objectives

Background

The U.S. Securities and Exchange Commission's (SEC) approximately 4,200 staff are located in 12 offices across the country. These offices include the agency's headquarters in Washington, D.C., and its 11 regional offices located in Atlanta, Boston, Chicago, Denver, Fort Worth, Los Angeles, Miami, New York, Philadelphia, Salt Lake City, and San Francisco. In addition to these 12 facilities – most of which are multi-tenant facilities that the SEC leases – the agency has 2 data centers located in Edison, New Jersey, and Beltsville, Maryland.

In February 2013, the Government Accountability Office updated its list of governmentwide high-risk areas.[1] According to the Government Accountability Office's report, Federal real property management remains a high-risk area, in part, because agencies continue to face challenges in protecting their Federal facilities.[2]

At the SEC, events in recent years indicated a need to examine the agency's program for safeguarding personnel, securing its facilities, and complying with Federal physical security standards. For example, in January 2011 the Office of Inspector General's (OIG) Office of Investigations (OI) completed an investigation into a contractor employee's ability to circumvent the SEC's physical security controls. The investigation found that the contractor employee, with the aid of SEC staff, was able to access the SEC's Operations Center[3] over a period of several weeks, although the agency had not completed the required background investigation of that employee.[4] Then, in January 2012, a contractor was able to allow an unauthorized person to enter the SEC's headquarters without the knowledge of SEC security staff. OI investigated the matter and identified several security vulnerabilities including:

- unmanned entry points that allowed SEC staff and contractors to bypass typical access control protocols after working hours; and

[1] Government Accountability Office, "High-Risk Series, An Update," GAO-13-283, February 2013.

[2] Executive Order 12977 (October 19, 1995), as amended by Executive Order 13286 (February 28, 2003), defines "Federal facilities" as "buildings and facilities in the United States occupied by Federal employees for nonmilitary activities."

[3] In September 2013, the SEC closed the Operations Center located in Alexandria, Virginia, and moved all personnel from that location to the agency's headquarters.

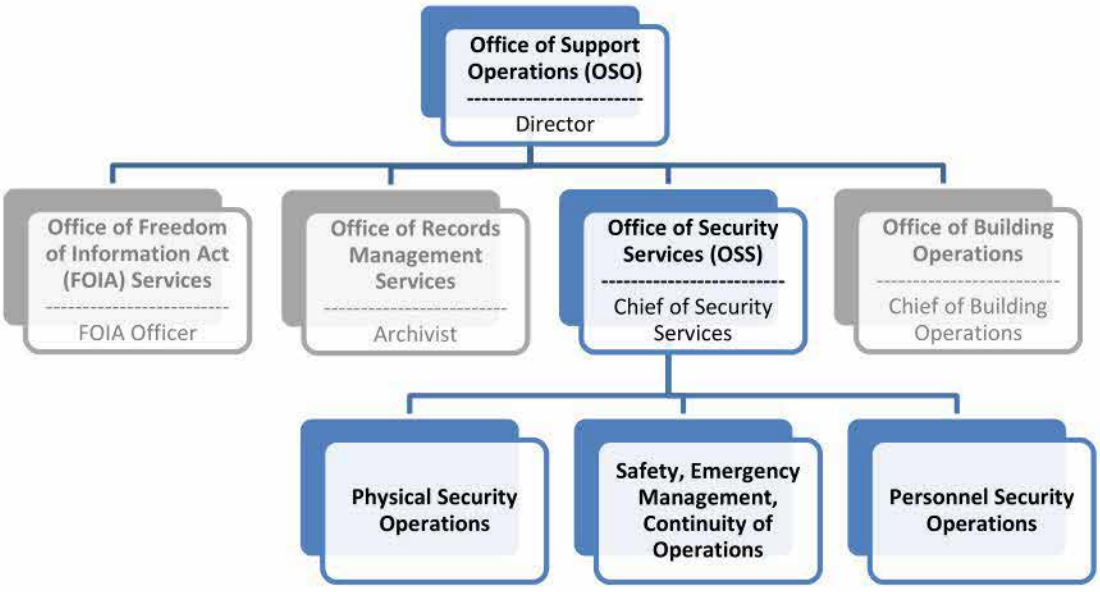
[4] U.S. Securities and Exchange Commission, Office of Inspector General, Case No. OIG-544, *OIT Contract Employees Given Access to SEC Buildings and Computer Systems for Several Weeks Before Background Investigation Clearance*, January 20, 2011. All four of the report's recommendations are closed.

- turnstiles that did not produce alarms in the SEC's security control center, which created the opportunity for unauthorized access without the knowledge of SEC security personnel.[5]

As a result of the OIG's investigations, agency management took action to improve the SEC's badge issuance processes and controlled entry points.

Security Services Roles and Responsibilities. The SEC's Office of Support Operations (OSO) is responsible for maintaining the security and safety of SEC staff and facilities, as well as for managing property, equipment, and overall building operations. Specifically, the Office of Security Services (OSS), under the direction of the Chief of Security Services and the OSO Director, is responsible for all operations related to physical security and safety of SEC staff and facilities. (See Figure below.) As of June 24, 2014, the OSS was staffed with 11 employees in the areas of physical security operations; safety, emergency management, and continuity of operations; and personnel security operations. The Physical Security Operations Branch was staffed with 3 employees (a branch chief and 2 physical security specialists) and 11 contractors (4 security specialists, 1 analyst, and 6 administrative personnel).

Figure. OSO Organizational Chart



Source: SEC internal website.

[5] Agency management stated that corrective action was taken to address the OIG's Report of Investigation, Case No. OIG-572, dated August 17, 2012; however, we were not able to determine whether the corrective actions fully addressed the identified risks.

To fulfill its responsibilities for day-to-day administration, monitoring, system maintenance, and operation of the SEC's access control, intrusion detection, and video monitoring systems, the OSS contracted with Kastle Systems (Kastle). Initiated in May 2011, the SEC's contract with Kastle provides for most of these activities to occur offsite.[6] In addition, the contract includes Monitoring Response Procedure agreements that specify when Kastle should notify SEC security personnel of alarm conditions. Depending on the nature of the alarm, Kastle notifies SEC security personnel by email, short message service (i.e., text message), or telephone.

Interagency Security Committee Standards, Best Practices, and Guidelines. Executive Order 12977 created the Interagency Security Committee (ISC) to enhance the quality and effectiveness of Federal facility security and protection.[7] The ISC, chaired by the Department of Homeland Security, establishes policies and develops and evaluates security standards and best practices for Federal facilities. ISC standards define the criteria and processes that security officials should use to determine facility security levels (FSL), and provide guidance for customizing Federal facility countermeasures. According to Executive Order 12977, "each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee." ISC standards apply to all nonmilitary Federal facilities in the United States, whether government-owned, leased, or managed; to be constructed or modernized; or to be purchased, including the SEC's facilities.

In August 2013, the ISC compiled previously distinct standards into a single source: the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (the ISC Risk Management Standard). This document provides an integrated source of physical security countermeasures for all nonmilitary Federal facilities.[8]

SEC Policies and Procedures. SEC policies and procedures provide guidance to employees and contractors and establish requirements for the agency's physical security program. Specifically, agency policies and procedures address topics including, but not limited to, physical access, key, and lock control; facility access cards; security clearances; contractor personnel entry and exit; electronic entry and exit systems; and workplace violence.[9]

[6] Kastle performs system monitoring, administration, and maintenance offsite. Card readers and cameras are provided onsite.

[7] Executive Order 12977, "Interagency Security Committee" (October 19, 1995), as amended by Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security" (February 28, 2003).

[8] Various ISC standards, best practices, and guidelines were applicable during the period of our audit. They are included in Appendix II.

[9] For the purposes of this report, "SEC policies and procedures" refers to SEC administrative policies, SEC policies, and SEC administrative regulations.

Objectives

To determine whether the SEC has effective policies and procedures, physical security measures, and internal controls to safeguard personnel and prevent unauthorized access to its facilities, the OIG contracted the services of Ollie Green & Company, CPA's, LLC (OG&C) (referred to as "we" in this report). OG&C's objectives were to assess

- the OSS' compliance with Federal physical security standards and SEC's policies and procedures;
- the effectiveness of the OSS' physical security policies and procedures; and
- the adequacy of the OSS' procedures and practices to oversee the physical security of the SEC's facilities.

To evaluate and assess the effectiveness of the SEC's physical security program, we conducted site visits at the SEC's headquarters in Washington, D.C., and at 3 of the agency's 11 regional offices: (1) the (b)(7)(F) (b)(7)(F) (b)(7)(F) We also performed site visits at the SEC's two data centers. Finally, we designed and sent to security personnel at all SEC facilities surveys requesting information about the agency's physical security program.

Appendices I, II, and III include additional information about our scope and methodology; our review of internal controls; prior audit coverage; the ISC standards, best practices, and guidelines; and the SEC's policies and procedures.

Results

Improvements Needed in the SEC's Physical Security Controls

We visited the SEC's headquarters, three of its regional offices (b)(7)(F) (b)(7)(F), and its two data centers, and obtained information from personnel at the remaining SEC facilities. From of our observations and the information we obtained, we determined that improvements are needed in the SEC's physical security controls. Specifically, we identified the following physical security vulnerabilities:

- facility risk assessments were incomplete, outdated, or not performed;
- facility security plans did not identify all current or planned security measures;
- SEC-issued badges were not always properly controlled;
- some access-controlled doors were unsecured; and
- the SEC's security system contractor (Kastle) monitored the agency's physical access control and intrusion detection systems from an offsite location, and did not always notify the OSS of alarm conditions.

In addition, the SEC's (b)(7)(F) lacked sufficient security measures to prevent unauthorized, undetected, and undocumented access to key information technology (IT) assets.

During the audit, management took action to address some of the conditions we observed; however, the conditions occurred because the OSS did not adequately manage and administer the SEC's physical security program. Specifically, we found that

- the OSS did not establish effective policies and procedures to address required Federal physical security standards;
- the OSS did not ensure that physical security program internal controls were measured and tested;
- security specialists' competencies did not always match their assigned roles and responsibilities; and
- the OSS outsourced security systems responsibilities to Kastle but did not provide sufficient oversight to monitor the contractor's performance.

The results of our audit indicate that action is required to establish a comprehensive physical security program and that doing so will reduce the risk to SEC personnel, facilities, and property.

SEC Risk Assessments Were Incomplete, Outdated, or Not Performed. Security risk assessments provide a methodology to assess a facility's risks against potential threats; however, we found that the SEC's facility risk assessments were incomplete, outdated, or not performed. Shortcomings in the agency's risk assessments may impact the agency's decision making. Because OSS assigned FSLs without conducting complete risk assessments, or updating risk assessment as necessary, the agency's decisions on achieving an adequate level of protection and necessary countermeasures might be impacted.

According to the ISC Risk Management Standard, a Federal facility's FSL serves as the basis for implementing protective measures. Sections 4.0 and 5.0 of the ISC Risk Management Standard supply the information and process required when designating an FSL to a Federal facility, including the process for designating an FSL to multi-tenant facilities such as the SEC's. As shown in Appendix IV, FSL determinations range from Level I (lowest risk) to Level V (highest risk), based on an assessment of the facility's mission criticality, symbolism, population, size, and threat. Once an FSL has been determined, departments and agencies follow a decision making process to identify an achievable level of protection that is commensurate with—or as close as possible to—the level of risk, without exceeding the level of risk. Specifically, security officials use the FSL to create a set of baseline standards that may be customized to address site-specific conditions. A baseline standard is a set of physical security countermeasures to be applied based on the facility's designated FSL.

The ISC Risk Management Standard states that FSL determinations should be made early enough in the space acquisition process to allow for the implementation of required countermeasures (or reconsideration of the acquisition caused by an inability to meet minimum physical security requirements). In addition, the ISC Risk Management Standard requires departments and agencies to conduct risk assessments as follows:

- at least once every 5 years for Level I and Level II facilities; and
- at least once every 3 years for Level III, Level IV, and Level V facilities.

Organizations must review and adjust FSLs, if necessary, as part of each initial and recurring risk assessment, and whenever a significant change occurs in the factors that impact a facility's FSL.

Where available, we reviewed the risk assessments and FSLs for the SEC's headquarters, 11 regional offices, and 2 data centers. As shown in Appendix V, we determined that many of the required assessments were incomplete, outdated, or not performed; and, overall, we were unable to determine whether the OSS followed the ISC Risk Management Standard when it assigned FSLs to the SEC's facilities. For

(b)(7)(E),(b)(7)(F)

According to the SEC's *Regional Office Site Physical Security Requirements*, dated November 4, 2013, the FSL for each of the above regional offices increased by one level. However, we found that the OSS had not updated the facilities' risk assessments, and the only FSL criteria used to change the FSL determinations was facility population. Such changes in FSLs should have triggered the performance of new facility risk assessments, which, in turn, may have led to needed changes in the facilities' protective measures.

In 2013, independent of the OSS risk assessments, the SEC's Office of Information Technology (OIT) conducted security risk assessments of the SEC's regional offices and data centers. However, the scope of the OIT's assessments was limited with respect to physical security controls. For example, the OIT's assessments were not required to include, nor did they include, an assessment of facility physical security controls measured against ISC standards. Rather, the OIT's assessments focused on requirements established by the National Institute of Standards and Technology and the Federal Information Security Management Act.

Facility Security Plans Did Not Identify All Current or Planned Security Measures. According to the ISC Risk Management Standard, facility security plans should identify current and planned security measures to mitigate threats against the facility and its occupants.[11] Such measures include but are not limited to placement of cameras, intrusion detection devices, security guard posts, and access control portals. After interviewing OSS staff and reviewing documentation for each facility visited, we determined that none of the SEC's facility security plans clearly and completely identified current or planned security measures. For example, during the site visit of the (b)(7)(E),(b)(7)(F) complete documentation of all security measures, the OSS may not be able to determine the effectiveness (or ineffectiveness) of such measures, or identify gaps in security coverage to provide a safe and secure environment for SEC personnel and to protect its facilities.

SEC-Issued Badges Were Not Always Properly Controlled. SEC facility access cards include credentials issued according to Homeland Security Presidential Directive 12 (HSPD-12),[12] SEC-issued badges, and employee and visitor passes. HSPD-12 credentials and SEC-issued badges are (b)(7)(F) (b)(7)(F) These types of facility access cards are issued to individuals after the OSS' Personnel Security Operations Branch has conducted a required background investigation and made a favorable

[11] The ISC Risk Management Standard, Appendix B, "Countermeasures," p. 49, further detailed on p. 76.

[12] Homeland Security Presidential Directive 12: *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

suitability determination. HSPD-12 credentials are issued to SEC personnel and contractors requiring physical access to SEC facilities for periods in excess of 180 days. SEC-issued badges are issued to persons requiring access for periods of less than 180 days.[13] Both types of cards allow unescorted electronic access to SEC facilities including access to controlled areas such as turnstiles, elevators, break areas, and stairwells. Passes (employee or visitor) (b)(7)(F) (b)(7)(F) but do not allow electronic access to SEC facilities, requiring visitors to be escorted at all times.

The SEC's *Facilities Access Card Policy* states, "SEC facilities access cards will be issued in accordance with prescribed policies which require the conducting of a background investigation, adjudication of the results, and issuance of identity credentials to employees and contractors who require access to Federally controlled facilities . . . ."[14] In addition, the policy addresses individuals who require short-term, unescorted access to SEC facilities and receive a suitability determination from the Personnel Security Operations Branch.[15]

During our visit to the (b)(7)(F) we determined that SEC staff created blank SEC-issued badges – without personnel photographs or identification information but programmed for access to SEC space – and issued the badges to persons that had not undergone the required background investigation. Many of the badges were issued to personnel such as janitorial staff and building engineers for periods exceeding 180 days. Staff at the (b)(7)(F) estimate that, from 2008 through December 2013, they issued to the commercial building owner and receptionist's desk about 50 of these badges without maintaining receipts or records of the individuals who received the badges. Once we reported this vulnerability to SEC management in the (b)(6),(b)(7)(C),(b)(7)(F) immediate action was taken to gain control of and accountability for the badges. However, by not following the requirements of the SEC's *Facilities Access Card Policy*, agency staff increased the risk that unauthorized individuals could gain access to SEC's controlled space without detection.

Some Access-Controlled Doors Were Unsecured. We conducted testing and walkthroughs of facility security access control points with SEC and contractor guard personnel present and found that some access-controlled doors were unsecured. The doors were in disrepair and permitted unauthorized access to controlled facilities, assets, and personnel. (b)(7)(E),(b)(7)(F)
(b)(7)(E),(b)(7)(F)

[13] SEC Administrative Policy, *Facilities Access Card Policy*, October 11, 2013.

[14] SEC Administrative Policy, *Facilities Access Card Policy*, p. 4.

[15] SEC Administrative Policy, *Facilities Access Card Policy*, p. 2.

(b)(7)(E),(b)(7)(F)

Appendix VI further describes the results of tests we performed on various doors at the facilities we visited, and the conditions we observed when conducting walkthroughs at those facilities.

[16] A door sweep is a small piece of plastic or rubber, attached to an aluminum carrier strip and fitted across the bottom of a door. It provides a weatherproof seal and prevents drafts from coming in under the door.

Kastle Monitored the SEC's Physical Access Control and Intrusion Detection Systems from an Offsite Location and Did Not Always Notify the OSS of Alarm Conditions. The ISC's *Security Systems Criteria* requires intrusion detection systems "monitor[ing] at an onsite central station during operating hours" for FSL IV facilities.[17] Although the OSS identified both the (b)(7)(F) (b)(7)(F) [18] we determined that, with the exception of the agency's data centers, Kastle monitored all of the SEC's physical access control and intrusion detection systems offsite.[19]

The SEC's contract with Kastle includes Monitoring Response Procedure agreements. Each agreement outlines select alarm conditions and procedures for when Kastle is required to notify SEC personnel. (b)(7)(F) (b)(7)(E),(b)(7)(F)

[17] The ISC Risk Management Standard, Appendix B, "Countermeasures," p. 43.

[18] See Appendix V, SEC Facility Security Risk Assessment and FSL Determinations.

[19] Data center monitoring activities are performed onsite. (b)(7)(F)

(b)(7)(F) **Lacked Sufficient Security Measures to Prevent Unauthorized, Undetected, and Undocumented Access to SEC IT Assets.** ISC standards require that Federal facility intrusion detection and access control systems be monitored and include controls to prevent and detect unauthorized and undocumented access to an organization's assets.[21]

(b)(7)(E),(b)(7)(F)

[21] The ISC Risk Management Standard, Appendix B, "Countermeasures," pp. 43 and 72. The ISC Risk Management Standard requires monitoring of access control and intrusion detection systems for Level I through IV facilities.

(b)(7)(F)

(b)(7)(E),(b)(7)(F)

The OSS Did Not Adequately Manage and Administer the SEC's Physical Security Program

The vulnerabilities we identified occurred because the OSS did not adequately manage and administer the SEC's physical security program. As described below, we found that the OSS did not:

- establish effective policies and procedures to address required ISC physical security standards;
- measure and test the SEC's physical security program internal controls; and
- ensure security specialists' competencies matched their assigned roles and responsibilities.

In addition, the OSS outsourced security systems responsibilities to Kastle but did not provide sufficient oversight to monitor the contractor's performance.

The OSS Did Not Establish Effective Policies and Procedures to Address Required ISC Physical Security Standards. We compared the OSS' physical security policies and procedures with the ISC standards, best practices, and guidelines, and determined that the agency's documents did not include all required Federal physical security standards. For example, Appendix E of the ISC Risk Management Standard requires Federal agencies to assess and document the effectiveness of their physical security programs through performance measurement and testing. The Standard further requires agencies to base performance measures on agency mission, goals, and objectives; and link performance results to goals and objectives development, resource needs, and program management.[24] However, as of May 29, 2014, the OSS had not established policies and procedures to address such requirements.

Additionally, although the SEC's *Physical Access, Key, and Lock Control Policy* references the ISC and states, "SEC access control requirements are governed by [HSPD-12] and [ISC] standards," we were unable to determine how the policy incorporated or reflected ISC standards.

[24] The ISC Risk Management Standard, Appendix E, "Use of Physical Security Performance Measures," pp. E-1 and E-2.

We reviewed the remaining SEC security policies and procedures[25] and were unable to identify any policies or procedures that reflect the required Federal standards established by the ISC. Because most of our work consisted of reviewing SEC security policies, procedures, assessments, and documentation from periods before August 2013, earlier ISC standards were applicable during the period of our audit. These standards have been incorporated into and superseded by the ISC Risk Management Standard established in August 2013, and include the following documents:

- *Facility Security Level Determinations for Federal Facilities*, An Interagency Security Committee Standard (For Official Use Only [FOUO]), (February 21, 2008).
- *Use of Physical Security Performance Measures* (June 2009).
- *Physical Security Criteria for Federal Facilities*, An Interagency Security Committee Standard, (FOUO) (April 12, 2010).
- *Child-Care Centers Level of Protection Template*, (FOUO) (May 2010/1st Edition).
- *Facility Security Committees*, An Interagency Security Committee Standard, (January 1, 2012/2nd Edition).
- The Design-Basis Threat, An Interagency Security Committee Report, (Unclassified//For Official Use Only [U//FOUO]) (April 2012).

However, we could not identify any SEC policies or procedures that incorporated these or any other physical security standards established by the ISC.

The OSS Did Not Always Measure and Test Physical Security Program Internal Controls. To assess and document the effectiveness of physical security programs, the ISC Risk Management Standard requires agencies to periodically measure and test their physical security controls.[26] However, we found that the OSS did not always measure and test the SEC's physical security internal controls. For example, (b)(7)(F) (b)(7)(E),(b)(7)(F) (b)(7)(F) By not measuring and testing its physical security controls to ensure compliance with SEC security policies and procedures and ISC standards, the SEC may be unaware of critical physical security controls that are not functioning as

[25] Appendix II lists the SEC policies and procedures that we reviewed.

[26] The ISC Risk Management Standard, Appendix E, pp. E-1 and E-2.

designed or intended. For example, as previously discussed and further described in Appendix VI, we observed several unsecured access-controlled doors in a state of disrepair and in need of attention. During our audit, OSS officials stated that they conducted informal measures and tests as resources permitted and are in the process of formalizing procedures and updating policies to include a measurement and testing program.

The OSS Did Not Ensure Security Specialists' Competencies Always Matched Assigned Roles and Responsibilities. Personnel competencies are critical to creating and managing a successful physical security program. The ISC's *Security Specialist Competencies* guideline provides the core competencies and general knowledge and skills a Federal security specialist should possess to perform their basic responsibilities.[27] The guideline also states a security specialist should understand the theory and application of physical protection systems with functions of detection, delay, and response. While various individuals (SEC employees and contractors) have served as security specialists over the last several years, we determined that three (one contractor and two employees) of the seven SEC security specialists[28] interviewed during the audit did not have the baseline level of knowledge, skills, and competencies necessary to effectively carry out their assigned roles and responsibilities.

To assess security specialists' basic knowledge and skills, we interviewed all seven and asked a series of questions about physical security countermeasures, such as intrusion detection and access control systems and testing of such countermeasures to ensure they function as intended. Answers provided by three of the specialists showed that they could not fully articulate the theory and application of physical protection systems. In most cases, the security specialists did not fully answer the questions. For some questions, the security specialists indicated that Kastle was responsible for performance of the task.

Without basic knowledge and skills, security specialists are unable to perform their duties and responsibilities for ensuring that adequate controls are in place and are measured and tested to safeguard SEC personnel and assets. For example, as of May 29, 2014, we determined that the OSS (including security specialists) did not take complete corrective actions to resolve the vulnerabilities we identified concerning the

(b)(7)(E),(b)(7)(F)

The OSS Outsourced Security Systems Responsibilities to a Third Party. The OSS outsourced a large part of its physical security systems responsibilities to Kastle but did not provide sufficient oversight to monitor the contractor's performance. For example, the failure to require onsite monitoring for the SEC's Level IV facilities

[27] *Security Specialist Competencies: An Interagency Security Committee Guideline*, 1st Edition, January 2012, p. 10, Section 4.14.

[28] For purposes of this audit security specialists were defined as security specialist I, II, and III; physical security specialists; and physical security supervisory security specialists and included SEC employees and contractors.

conflicts with ISC standards. This may be a reflection of the competencies of the security specialists, as previously discussed. The OSS' management of the contract with Kastle resulted in shortcomings in the security posture of the SEC's facilities;

(b)(7)(E),(b)(7)(F)

Conclusion

The OSS is responsible for implementing, maintaining, and overseeing effective security measures at all SEC facilities and maintaining the security and safety of SEC employees and contractors. However, we found that the OSS did not comply with governing Federal physical security standards and some SEC policy and procedures. We also found that the OSS' physical security policies and procedures were insufficient and ineffective as they did not reflect all required ISC standards and were not always followed and enforced. Finally, because of the weaknesses in the OSS' policies and procedures, the organization's internal controls for and oversight of the SEC's physical security program were not adequate.

We identified physical security vulnerabilities that increased the SEC's risk to its personnel, facilities, and property. Although agency management took corrective action to address some of the specific conditions observed during the audit, we believe that additional attention is required to establish a comprehensive physical security program and to reduce the SEC's risk.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's physical security controls and establish a comprehensive physical security program, the Office of Security Services should implement the following recommendations:

Recommendation 1: Revise the SEC's physical security policies and procedures to reflect Interagency Security Committee standards, including requirements for (a) facility security level determinations and risk assessments; (b) identification of current and planned security measures; (c) onsite monitoring of physical access control and intrusion detection systems for facility security level IV facilities; and (d) periodic measuring and testing of security controls.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 2: Conduct or update risk assessments and implement appropriate corresponding protective measures for the SEC's headquarters, data centers, and regional offices, in accordance with Interagency Security Committee standards.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 3: Review the facility security plans for all SEC facilities and revise the plans as necessary to include current and planned security measures, as required by Interagency Security Committee standards.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 4: Verify that (a) only authorized personnel with favorable suitability determinations have been provided SEC-issued badges; and that (b) badge expiration dates have not exceeded 180 days from the date of issuance and take corrective action to address any discrepancies found, in accordance with the SEC's facilities access card and security clearance policies.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 5: Take immediate actions to ensure that all access-controlled doors are operating effectively. These actions should include, but are not limited to,

- (b)(7)(F)
- establishing a system to periodically test all access-controlled doors for operational functionality and correct any deficiencies found.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 6: Coordinate with the Office of Acquisitions to assess the contract with Kastle Systems and revise the contract as necessary to (a) ensure that alarm notification protocols meet the SEC's business needs, provide adequate protection of SEC personnel and assets, and reflect facility security level determinations; and (b) provide onsite monitoring of the SEC's facility security level IV facilities.

Management's Response. The Director, Office of Support Operations, did not fully concur with the recommendation because there was no documented, supported change to the facility security level determination in 2013. Nevertheless, the Director stated that the Office of Security Services is in the process of conducting facility level determinations and will evaluate monitoring and notification procedures for SEC facilities to ensure compliance with Interagency Security Committee processes and guidelines. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. As stated in the report, during the audit we obtained a written document entitled, *Regional Office Site Physical Security Requirements*, dated November 4, 2013, that identified changes in the facility security level determinations for the SEC's (b)(7)(F) (b)(7)(F) However, because management is in the process of conducting facility security level determinations, we revised the recommendation by removing the reference to the 2013 facility security level determinations. Management's actions are responsive to the intent of the recommendation; therefore, the recommendation is resolved and will be closed upon completion and verification of the actions taken.

Recommendation 7: Conduct a thorough review of the physical security controls at the (b)(7)(F) mitigate any vulnerabilities identified, including vulnerabilities previously identified by the Office of Information Technology; and assign facility security levels.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 8: Coordinate with the Office of Acquisitions and Office of Information Technology to ensure that all physical security contract requirements for the (b)(7)(F) are being met, to include (b)(7)(F) (b)(7)(F)

Management's Response. The Director, Office of Support Operations, concurred with the recommendation and stated that the Office of Security Services will collaborate with the Office of Information Technology to review the physical security controls, determine vulnerabilities, and mitigate risk to ensure facilities the Office of Information Technology has contracted with are in compliance of the Interagency Security Committee's recommendations. Further, the Office of Information Technology and the Office of Acquisitions will coordinate to ensure contract requirements are met. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. As a result of management's response, we revised the recommendation by specifying that the Office of Security Services should coordinate with the Office of Acquisitions and Office of Information Technology to ensure that all ***physical security*** contract requirements for the (b)(7)(F) are being met. Management's proposed actions are responsive to the intent of the recommendation; therefore, the recommendation is resolved and will be closed upon completion and verification of the actions taken.

Recommendation 9: Provide training for security specialists and other physical security personnel to ensure they possess a baseline knowledge of physical security standards and core competencies.

Management's Response. The Director, Office of Support Operations, concurred with the recommendation. Management's complete response is reprinted in Appendix VII.

OIG's Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Appendix I. Scope and Methodology

Ollie Green & Company, CPAs, LLC, conducted this performance audit from September 2013 through July 2014 in accordance with generally accepted government auditing standards.[29] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our overall objective was to determine whether the SEC has effective policies and procedures, physical security measures, and internal controls to safeguard personnel and prevent unauthorized access to its facilities. Specifically, we assessed

1. the OSS' compliance with Federal physical security standards and SEC policies and procedures;

2. the effectiveness of the OSS' physical security policies and procedures; and

3. the adequacy of the OSS' procedures and practices to oversee the physical security of the SEC's facilities.

Scope. We conducted the audit from September 2013 to July 2014 and included a review of SEC's policies, procedures, risk assessments, physical security measures, and internal controls in place at the SEC's headquarters, 11 regional offices, and 2 data centers during fiscal years 2012 and 2013 through January 2014. The scope was limited to reviewing OSO's internal controls and assessing whether effective physical security controls exist to prevent unauthorized access to SEC facilities. The scope further included determining whether the SEC's physical security controls were in compliance with Federal physical security standards, best practices, and guidelines, and SEC policy and procedures. Appendices II and III list the relevant standards, best practices, and guidelines and SEC policies and procedures for physical security that we reviewed.

Methodology. To determine whether the SEC has effective physical security policies and procedures, physical security measures, and internal controls to safeguard personnel and prevent unauthorized access to its facilities, we first gained an understanding of the SEC's physical security program. We identified Federal physical security standards. In addition, we examined documents and records related to the physical security programs of each SEC facility and reviewed the OSS' physical security policies, procedures, and internal controls. Also, we compared agency policies and procedures to required Federal physical security standards established by the ISC.

[29] To obtain subject matter expertise in the area of physical security, Ollie Green & Company, CPAs, LLC, subcontracted with X7 Systems Integration.

Additionally, we conducted site visits at 3 of the agency's 11 regional offices: (1) the (b)(7)(F)

We defined and quantified risk in terms of the size of each facility, the number of SEC and contractor personnel present, the perimeter security features, the history of crime in each facility, each facility's FSL, and whether visitors were required to be escorted. We also performed site visits at the SEC's headquarters in Washington, D.C., and the agency's two data centers located in (b)(7)(F) At each location visited, we conducted interviews of SEC and contractor personnel and observed physical security practices. We also conducted walkthroughs to locate and assess the condition of CCTV systems, access control systems, intrusion detection systems, and other physical security equipment. To determine whether alarm systems were operating properly, we propped open and forced open doors. Finally, we designed and sent surveys to all SEC facility directors, including those at the eight regional offices we did not visit, requesting information about their physical security programs. Such information included security points of contacts, organizational charts, manning schedules, guard force information, training information, floor plans, and risk assessments.

Internal Controls. To identify and assess internal controls relevant to our audit objectives, we interviewed OSS personnel, and reviewed available physical security policies, procedures, and standards. In planning and performing our audit, we considered whether internal controls significant to the audit were properly designed and implemented. In addition, we obtained an understanding of the internal controls associated with the implementation of Federal standards and determined whether the SEC implemented internal controls. We confirmed our understanding of these controls and procedures through interviews and analysis of applicable documents.

Prior Audit Coverage. We determined through interviews of OSS management personnel and independent research that no physical security audits had been conducted in recent years; therefore, follow-up procedures were not applicable.

Use of Computer-Generated Data. In conducting our audit, we did not rely on computer-generated data; therefore, the sufficiency and reliability of such data was not applicable in meeting the audit objectives.

Appendix II. ISC Standards, Best Practices, and Guidelines

The ISC's standards, best practices, and guidelines are designed for Federal security professionals responsible for protecting nonmilitary Federal facilities in the United States. The documents help such professionals implement security policies and mandatory standards.

ISC Standards. The ISC's *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard – August 2013/1st Edition* (the ISC Risk Management Standard) defines the criteria and processes that those responsible for a facility's security should use in determining its security level and provides an integrated, single source of physical security countermeasures for all nonmilitary Federal facilities. It also provides guidance on countermeasure customization for Federal facilities. The ISC Risk Management Standard supersedes previous standards and guidance and includes the following sections:

- **Section 1.0: The Interagency Security Committee Risk Management Process** provides an introduction to the risk management process and outlines the approach necessary to identify, assess, and prioritize the risks to Federal facilities.

- **Section 2.0: Background** provides a review of the foundational documents that codify the Department of Homeland Security's responsibility for protecting buildings, grounds, and property that are owned, occupied, leased, or secured by the Federal Government.

- **Section 3.0: Applicability and Scope** outlines the authority of the ISC and the Standard.

- **Section 4.0: Facility Security Level Determinations for Federal Facilities** supplies the information and process required when designating an FSL to a Federal facility. The FSL is then used to create a set of baseline standards that may be customized to address site-specific conditions.

- **Section 5.0: Integration of the Physical Security Criteria** provides an overview of how the application of physical security criteria is predicated on an FSL designation. Once an FSL has been determined, departments and agencies follow a decision making process outlined in this section to identify an achievable level of protection that is commensurate with—or as close as possible to—the level of risk, without exceeding the level of risk.

Section 6.0: The Risk Informed Decision-Making Process summarizes a process of identifying and implementing the most cost-effective countermeasure appropriate for mitigating vulnerability, reducing the risk to an acceptable level.

The ISC Risk Management Standard also incorporates appendices, which had been previously established as separate ISC standards. During the period under review, these standards were as follows:

- *Facility Security Level Determinations for Federal Facilities*, An Interagency Security Committee Standard (FOUO), (February 21, 2008).
- *Use of Physical Security Performance Measures* (June 2009).
- *Physical Security Criteria for Federal Facilities*, An Interagency Security Committee Standard, (FOUO) (April 12, 2010).
- *Child-Care Centers Level of Protection Template*, (FOUO) (May 2010/1st Edition).
- *Facility Security Committees*, An Interagency Security Committee Standard, (January 1, 2012/2nd Edition).
- The Design-Basis Threat, An Interagency Security Committee Report, (U//FOUO) (April 2012).

ISC Best Practices. In addition to issuing Federal physical security standards, the ISC has issued the following best practices:

- *Best Practices for Armed Security Officers in Federal Facilities – April 2013/2nd Edition* – This document recommends a set of minimum standards to be applied to all contract armed security officers assigned to U.S. buildings and facilities occupied by Federal employees for nonmilitary activities.
- *Violence in the Federal Workplace: A Guide for Prevention and Response – April 2013/1st Edition* – This guide provides important information to assist department and agency security planners in addressing acts of violence in the workplace.
- *Occupant Emergency Programs: An Interagency Security Committee Guide – March 2013/1st Edition* – This guide assists department and agency security planners in developing and reviewing Occupant Emergency Programs for the safety and security of employees and visitors at nonmilitary Federal facilities.
- *Best Practices for Managing Mail Screening and Handling Processes: A Guide for the Public and Private Sectors (NON-FOUO) – September 2012/1st Edition* – This document provides best practices for the screening and handling of all incoming packages and letters, whether delivered via the United States Postal Service, commercial common couriers, or special messengers.

- *Combating Terrorism Technical Support Office, Technical Support Working Group/ISC - Best Practices for Mail Screening and Handling (FOUO) – September 2011/1st Edition* – This guide provides mail center managers, their supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to an organization by its received and delivered mail and packages.

ISC Guidelines. The ISC also issued the following guidelines:

***Security Specialist Competencies*, An Interagency Security Committee Guideline, (January 2012, 1st Edition).** The ISC issued this guidance to provide the range of core competencies that Federal security specialists can possess to perform their basic duties and responsibilities. The document states that incumbents will be knowledgeable in all respective agency policy and standards, as well as those issued by the ISC.

Appendix III. SEC Policies and Procedures

The SEC has designed policies and procedures to protect personnel and safeguard SEC assets. These policies include the following:

SEC Policy, *Physical Access, Key, and Lock Control Policy*, May 30, 2013. This policy provides guidance and explains how personnel are granted physical access to an area within an SEC facility. SEC access control requirements are governed by HSPD-12 and ISC standards.

SEC Administrative Policy, *Facilities Access Card Policy*, October 11, 2013. This document prescribes policies and standards governing the SEC's facilities access cards. It prescribes the use of facilities access cards and explains who is responsible for their issuance, maintenance, and control. Facility access cards include HSPD-12 credentials, SEC-issued badges, and employee and visitor passes.

SEC Administrative Policy, *Group Visitor Admittance Policy*, July 2012. This policy establishes a uniform Group Visitor Admittance program and service for the SEC. It explains the visitor process, responsibilities of the host and visitors while in an SEC facility, and the proper use of visitor passes. The policy refers to headquarters only. SEC regional offices shall follow the process and procedures of their building management.

SEC Administrative Regulation, SECR 23-3 (Rev. 1), *Security Clearance Policy*, October 11, 2012. This regulation prescribes the SEC's policies, procedures, and responsibilities for requesting security clearances and the procedures for processing requests. The regulation applies to all SEC staff, including fellows, interns, contractors, and anyone employed on a full-time or part-time basis by the SEC.

SEC Administrative Regulation, SECR 23-2a, *Safeguarding Non-Public Information*, January 21, 2000. This regulation establishes the SEC's general policies and procedures for safeguarding non-public information. The regulation applies to all SEC personnel.

Appendix IV. Process for Determining FSLs

According to the ISC Risk Management Standard, the process for managing Federal facility risk begins with determining the FSL according to the characteristics of each facility and the Federal occupant(s). As shown in the FSL matrix below, the five equally weighted factors quantified to determine an FSL are mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. In addition, a sixth factor – intangibles – allows assessors to consider other factors unique to the department's or agency's needs or to the facility itself.

Table 1. Factors for Determining FSL Levels[30]

Factor	Points				Score
	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	<100	101-250	251-750	>750	
Facility Size	<10,000 sq. ft.	10,001-100,000 sq. ft.	100,001-250,000 sq. ft.	>250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	I 5-7 Points	II 8-12 Points	III 13-17 Points	IV 18-20 Points	Preliminary FSL
Intangible Adjustment	Justification:				+/- 1 FSL
					Final FSL

Source: *Facility Security Level Determinations for Federal Facilities,* An Interagency Security Committee Standard, p. 6, August 2013.

[30] The ISC Risk Management Standard, p. 14 states, "As general guidance, agencies should consider a facility as potentially suitable for a Level V designation if it receives a 'very high' score value for criticality or symbolism and is a one-of-a-kind facility (or nearly so)."

The five tangible FSL factors are listed and further described in the ISC Risk Management Standard, along with examples and criteria for how they scored:

1. **Mission Criticality**
   Example: Level "Very High" with Score of 4 - Houses personnel or specialized equipment essential to regulating national fiscal or monetary policy, financial markets, or other economic functions.

2. **Symbolism**
   Example: Level "Very High" with Score of 4 - Executive department headquarters building.

3. **Facility Population**

Value	Points	Criteria
Very High	4	Greater than 750 occupants or facilities with childcare centers
High	3	Between 251 and 750 occupants
Medium	2	Between 101 and 250 occupants
Low	1	Less than 100 occupants

4. **Facility Size**

Value	Points	Criteria
Very High	4	Greater than 250,000 sq. ft.
High	3	Between 100,000 and 250,000 sq. ft.
Medium	2	Between 10,000 and 100,000 sq. ft.
Low	1	Up to 10,000 sq. ft.

5. **Threat to Tenant Agencies**
   Example: Level "Medium" with Score of 2 – Generally, nonadversarial public contact according to the nature of business conducted at the facility.

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

(b)(7)(E),(b)(7)(F)

Appendix VII. Management Comments

OFFICE OF SUPPORT OPERATIONS

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

MEMORANDUM

July 30, 2014

TO: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects, Office of Inspector General

FROM: Barry D. Walters, Director, Office of Support Operations Barry D Walters

SUBJECT: *Audit of the SEC's Physical Security Program*, Report No. 523 (Draft)

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 523, *Audit of the SEC's Physical Security Program*. Thank you for the opportunity to review and respond to this report. We concur with a majority of the recommendations in the audit report and will implement them as resources permit.

Recommendation 1: Revise the SEC's physical security policies and procedures to reflect Interagency Security Committee standards, including requirements for (a) facility security level determinations and risk assessments; (b) identification of current and planned security measures; (c) onsite monitoring of physical access control and intrusion detections systems for facility security level IV facilities; and (d) periodic measuring and testing of security controls.

The Office of Support Operations concurs with this recommendation.

Recommendation 2: Conduct or update risk assessments and implement appropriate corresponding protective measures for the SEC's headquarters, data centers, and regional offices, in accordance with Interagency Security Committee standards.

The Office of Support Operations concurs with this recommendation.

Recommendation 3: Review the facility security plans for all SEC facilities and revise the plans as necessary to include current and planned security measures, as required by Interagency Security Committee standards.

The Office of Support Operations concurs with this recommendation.

Recommendation 4: Verify that (a) only authorized personnel with favorable suitability determinations have been provided SEC-issued badges; and that (b) badge expiration dates have not exceeded 180 days from the date of issuance and take corrective action to address any

discrepancies found, in accordance with the SEC's facilities access card and security clearance policies.

The Office of Support Operations concurs with this recommendation.

Recommendation 5: Take immediate actions to ensure that all access-controlled doors are operating effectively. These actions should include, but are not limited to;

- (b)(7)(F)
- establishing a system to periodically test all access-controlled doors for operational functionality and correct any deficiencies found.

The Office of Support Operations concurs with this recommendation.

Recommendation 6: Coordinate with the Office of Acquisitions to assess the contract with Kastle Systems and revise the contract as necessary to (a) ensure that alarm notification protocols meet the SEC's business needs, provide adequate protection of SEC personnel and assets, and reflect the 2013 change in facility security level determinations; and (b) provide onsite monitoring of the SEC's facility security level IV facilities.

The Office of Support Operations does not fully concur with this recommendation. (b)(7)(F)
(b)(7)(F)

Recommendation 7: Conduct a thorough review of the physical security controls at the (b)(7)(F) mitigate any vulnerabilities identified, including vulnerabilities previously identified by the Office of Information Technology; and assign facility security levels.

The Office of Support Operations concurs with this recommendation.

Recommendation 8: Coordinate with the Office of Acquisitions and Office of Information Technology to ensure that all contract requirements for the (b)(7)(F)
(b)(7)(F)

The Office of Support Operations concurs with this recommendation, however as discussed and agreed to with Ms. Sharek on July 18, it is outside the purview of the OSS to ensure all contract

requirements of an Office of Information Technology (OIT) contract are being met. The OSS will collaborate with the OIT to review the physical security controls, determine vulnerabilities, and mitigate risk to ensure facilities OIT has contracted with are within compliance of ISC recommendations. The OIT and the Office of Acquisitions will coordinate to ensure contract requirements are met.

Recommendation 9: Provide training for security specialists and other physical security personnel to ensure they possess a baseline knowledge of physical security standards and core competencies.

The Office of Support Operations concurs with this recommendation.

Appendix VIII. OIG Response to Management Comments

We are pleased that the Director, Office of Support Operations, fully concurred with eight of the nine recommendations. Management's response to Recommendations 1 through 5, 7, and 9, did not describe planned corrective action. Therefore, we will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendations. The recommendations will remain open until completion and verification of appropriate corrective action.

As a result of management's response to Recommendation 8, we modified the recommendation by specifying that the Office of Security Services should coordinate with the Office of Acquisitions and Office of Information Technology to ensure that all ***physical security*** contract requirements for the (b)(7)(F) are being met. Management's proposed actions are responsive to the recommendation; therefore, the recommendation is resolved and will be closed upon completion and verification of the actions taken.

Because management is in the process of conducting facility security level determinations, we revised Recommendation 6 by removing the reference to the 2013 facility security level determinations. Although management did not fully concur with the recommendation, the proposed corrective actions are responsive to the intent of the recommendation; therefore, the recommendation is resolved and will be closed upon completion and verification of the actions taken.

To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

E-mail: oig@sec.gov

Telephone: (877) 442-0854

Fax: (202) 772-9265

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549-2736

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6083. Comments, suggestions, and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.