U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement

June 15, 2018

Report No. 547

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

June 15, 2018

TO: Stephanie Avakian, Co-Director, Division of Enforcement
Steven Peikin, Co-Director, Division of Enforcement
Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement*, Report No. 547

Attached is the Office of the Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) internal controls for retaining external experts and foreign counsel for the Division of Enforcement. The report contains seven recommendations for corrective action that, if fully implemented, should improve (1) oversight of contracts for expert services, and (2) the SEC's ability to address information security risks inherent in the Division of Enforcement's contracts for expert services.

On June 1, 2018, we provided management with a draft of our report for review and comment. In its June 7, 2018, response, management concurred with our recommendations. We have included management's response as Appendix II 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 the agency will address the recommendations.

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

Attachment

cc: Jay Clayton, Chairman
Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Michael S. Piwowar, Commissioner
Richard Grant, Counsel, Office of Commissioner Piwowar
Robert J. Jackson Jr., Commissioner

Caroline Crenshaw, Counsel, Office of Commissioner Jackson
Prashant Yerramalli, Counsel, Office of Commissioner Jackson
Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Robert B. Stebbins, General Counsel
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Rick A. Fleming, Investor Advocate
Vance Cathell, Director, Office of Acquisitions
Gregory Steigerwald, Competition Advocate, Office of Acquisitions
Bridget Fitzpatrick, Chief Litigation Counsel, Division of Enforcement
David Gottesman, Deputy Chief Litigation Counsel, Division of Enforcement
Margaret McGuire, Senior Counsel to the Co-Directors, Division of Enforcement
Wanda Armwood, Assistant Director, Division of Enforcement
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Audit of the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement
Report No. 547
June 15, 2018

Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) Division of Enforcement (ENF) conducts investigations into possible violations of Federal securities laws and litigates the SEC's civil enforcement proceedings in Federal courts and in administrative proceedings. ENF routinely retains outside experts—attorneys, accountants, economists, and other professionals—and foreign counsel (collectively referred to hereafter as "experts") to fulfill a variety of roles during investigations and litigation. Between April 1, 2015, and March 31, 2017, the SEC awarded almost 200 contracts for expert services totaling more than $35 million. So that experts can fulfill contract requirements, ENF may provide experts sensitive, non-public information, including information that is personally identifiable, commercially valuable, and market-sensitive. We conducted this audit to determine whether the SEC implemented effective controls for (1) reviewing and approving requests for expert services, including selecting experts; and (2) managing contracts with experts and the funds spent on experts' services, fees, and expenses.

What We Recommended

We made seven recommendations, including that management develop guidance to help CORs more effectively monitor work performed under contracts for expert services; develop a process that ensures contracting officers enforce contract requirements related to PII when necessary; and implement a standardized process to verify NDA receipt for individuals who will perform work under contracts for expert services. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

What We Found

Since March 2015, ENF has improved its process for submitting and approving requests for expert services. We judgmentally selected and reviewed 21 of ENF's 197 contracts for expert services awarded during our scope period and determined that the internal controls for reviewing and approving requests and for selecting experts were operating effectively. In addition, although we identified small amounts over-billed to the SEC because of inadequate contract management, we did not identify fraud, waste, or significant mismanagement of the funds spent on the experts' services, fees, and expenses we reviewed. However, the SEC can better manage ENF's contracts for expert services.

To help contracting officers' representatives (CORs) monitor the contracts, the SEC required experts to submit monthly status reports. Experts generally did not submit these reports, and agency personnel did not enforce the requirement to do so. In addition, some experts submitted invoices with little to no detail about the work performed and the personnel who performed it. Because CORs for the contracts we reviewed had limited first-hand knowledge of the sufficiency of contract deliverables and work performed, they were unable to determine whether invoices accurately reflected work performed. Instead, CORs relied on ENF attorneys for that determination. As a result, CORs' ability to conduct surveillance of contractors' performance was limited.

Moreover, although the SEC established some requirements in recognition of certain information security risks, agency personnel did not always enforce those requirements. For example, more than half of the 113 individuals reported as having worked on the contracts we reviewed either had not signed the required non-disclosure agreement (NDA) or had signed one after beginning work. For one contract we reviewed, 11 of 12 NDAs on file were signed, on average, 305 days after individuals began work. The remaining six individuals who performed work under the contract had not signed an NDA. In addition, in at least five instances, agency personnel had not enforced contract requirements related to safeguarding personally identifiable information (PII) even though experts had access to PII, including investors' names, addresses, dates of birth, and customer account information. We also found that contracts lacked controls regarding the inadvertent release or disclosure of information after the SEC transmits information to experts. As a result, the agency lacked assurance that experts and their information systems achieved basic levels of security to protect the SEC's sensitive, non-public information, including PII. We did not identify instances in which unauthorized individuals accessed such information after it was provided to experts. However, the agency should take steps to minimize the risk of unauthorized disclosure, modification, and use of its sensitive, non-public information provided to experts.

For additional information, contact the Office of Inspector General at (202) 551-6061 or https://www.sec.gov/oig.

TABLE OF CONTENTS

ABBREVIATIONS

COR	contracting officer's representative
CP	contractor personnel
ENF	Division of Enforcement
FAR	Federal Acquisition Regulation
NDA	non-disclosure agreement
OA	Office of Acquisitions
OIG	Office of Inspector General
PII	personally identifiable information
SEC or agency	U.S. Securities and Exchange Commission
SECR	U.S. Securities and Exchange Commission Administrative Regulation
T&M/LH	time-and-materials and labor-hour

Background and Objectives

Background

The U.S. Securities and Exchange Commission's (SEC or agency) Division of Enforcement (ENF) conducts investigations into possible violations of Federal securities laws and litigates the SEC's civil enforcement proceedings in Federal courts and in administrative proceedings. ENF routinely retains outside experts and foreign counsel (collectively referred to hereafter as "experts") in its enforcement activities to fulfill a variety of roles, depending on the type or stage of a case.[1] Experts may be attorneys, accountants, economists, or other professionals who are self-employed or employed by firms, companies, universities, or other entities. Typically, experts work remotely, do not have access to SEC facilities, and are not provided SEC e-mail accounts or access to the agency's network. The nature of an expert's work depends on the circumstances and the requirements of the respective court and location of the court's jurisdiction, either domestic or international. So that experts can fulfill contract requirements, ENF may provide experts sensitive, non-public information, including information that is personally identifiable, commercially valuable, and market-sensitive. Because ENF cannot predict the pace of its investigations or litigation, or what additional (or less) support will be needed as cases proceed, the SEC's contracts with experts describe in general terms the work to be performed. According to the SEC, given the significance and complexity of the work experts perform, firm-fixed-price or fixed-price with economic price adjustment contracts are not practical. Instead, the SEC uses time-and-materials and labor-hour (T&M/LH) contracts for expert services. As shown in Table 1, between April 1, 2015, and March 31, 2017, the SEC awarded 197 contracts for expert services equal to or greater than $1,000[2] and totaling more than $35 million.[3]

According to SEC Administrative Regulation (SECR) 10-17, *Time-and-Materials and Labor-Hour Contracts* (Rev. 1; August 20, 2015) (SECR 10-17),[4] the SEC limits, to the maximum extent possible, its use of T&M/LH contracts. T&M/LH contracts expose the Government to the greatest amount of risk because the Government pays the

[1] ENF retains foreign counsel primarily to represent the SEC's interests in foreign courts.

[2] According to agency records, five contracts for expert services for less than $1,000 were awarded during our scope period (April 1, 2015, to March 31, 2017). Based on materiality, we did not include these five contracts in the audit population.

[3] The SEC's Office of Acquisitions (OA) is responsible for the execution and management of all agency acquisitions, including contracting for experts.

[4] SECR 10-17 prescribes policies and procedures for the agency's proper use and administration of T&M/LH contracts. Although the SEC released the current version of SECR 10-17 after the commencement of the audit period (April 1, 2015), we confirmed that the prior version of the policy (released February 18, 2011) was substantially the same.

contractor for time delivered rather than a measurable product with measurable quality attributes. As such, contracting officers, contracting officers' representatives (CORs),[5] and all other SEC employees involved in the award should work together to ensure compliance with the requirements of the contract. Contracts for expert services generally delineate requirements for ENF attorneys, contracting officers, and CORs.[6]

Table 1. Contracts for ENF Expert Services Equal to or Greater than $1,000 Awarded Between April 1, 2015, and March 31, 2017

SEC Office	Total No. of Contracts	Total Contracted Amount
Headquarters	55	$10,969,136
Atlanta	10	$2,507,625
Boston	5	$696,635
Chicago	9	$2,190,190
Denver	27	$5,980,113
Fort Worth	9	$1,956,620
Los Angeles	16	$3,798,541
Miami	10	$1,280,295
New York	28	$3,199,835
Philadelphia	7	$866,050
Salt Lake	9	$1,655,157
San Francisco	12	$549,212
TOTAL	**197**	**$35,649,409**

Source: Office of Inspector General (OIG)-generated using financial data obtained from the Office of Financial Management and OIG queries of the agency's contracting system.

In March 2015, ENF began using SharePoint to automate its process for requesting experts.[7] Once an ENF attorney identifies a need for an expert and conducts market

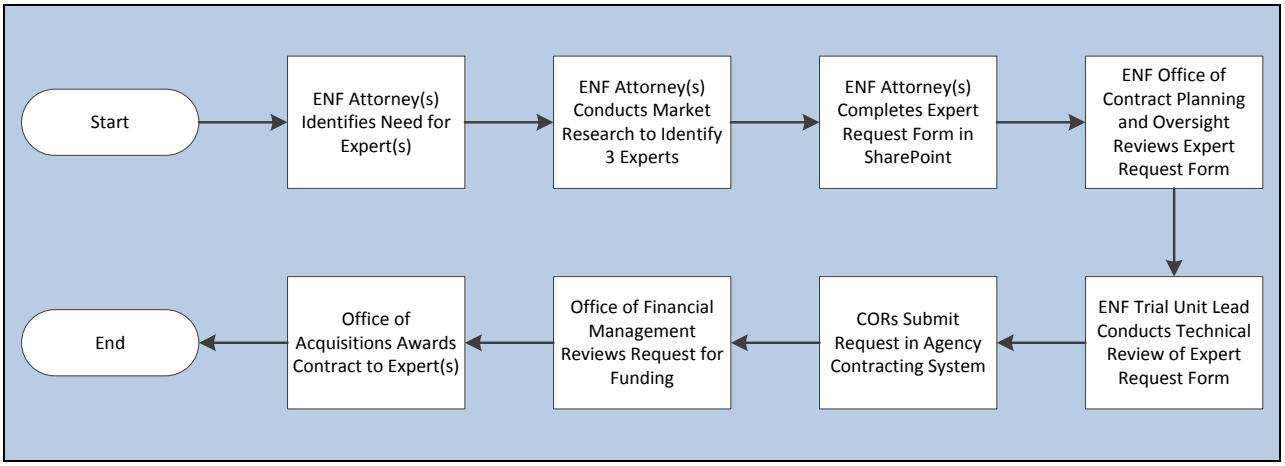
[5] Contracting officers are required to appoint, in writing, a COR for each contract. Pursuant to SECR 10-15, *Contracting Officer's Representative*, the COR is an employee, "with technical knowledge and understanding to carry out the terms of the specified contract." Generally, CORs for ENF's contracts for expert services are program support specialists assigned to each SEC regional office. The COR assigned to the agency's Headquarters is the Lead Program Management Analyst who assists CORs from the regional offices as needed.

[6] Generally, contracts for expert services name an ENF attorney working on the case as the individual responsible for inspecting and accepting services furnished under the contract. The COR is charged with managing the contract in coordination with the contracting officer and within the terms of the contract, to include reviewing contractor invoices and charges.

[7] Before March 2015, ENF used a centralized system of manually tracking requests for expert services, which resulted in potential delays in retaining experts.

research to identify potential experts,[8] the attorney completes in SharePoint an expert request form. The form captures, among other things, details about the corresponding ENF case, a justification for hiring an expert, information about the requested expert as well as the other experts considered, and whether the requested expert is registered in the System for Award Management.[9] ENF's Office of Contract Planning and Oversight conducts an administrative review of the attorney's request. If the Office of Contract Planning and Oversight approves the request, the ENF Trial Unit Lead conducts a second-level review. If the Lead approves the request, the SEC's Office of Financial Management determines whether funding is available and, if so, OA awards a contract to the expert. The figure below shows the SEC's end-to-end process for retaining experts.

Figure. SEC Process for Retaining Experts



Source: OIG-generated using ENF's *Retaining Expert Services and Consultants* (June 2017).

The SEC's contracts for expert services follow standard template language and generally include the following requirements:

Status Reports. The contractor shall submit a monthly status report, via e-mail, of all work performed under the contract by the 15th of each month. The progress report shall contain, among other things: (1) a summary of progress during the reporting period, including any significant technical information; (2) unanticipated technical or management problems of significance; (3) a summary of important meetings, briefings, trips, and conferences; (4) labor hours used versus labor hours planned per task (both

[8] ENF attorneys must consider a minimum of three experts and select the most appropriate candidate who does not have a conflict of interest (either general subject matter conflicts or entity conflicts).

[9] The System for Award Management is the Federal Government's primary database for procurement and payment information and is designed to streamline the payment process and facilitate paperless payments through electronic funds transfer. Contracting officers are generally prohibited from awarding contracts to vendors who do not have an active registration in the system.

for the reporting period and cumulatively for the entire contract); and (5) a statement of projection (budget) for the next reporting period.

Submission of Invoices. Contractors should submit invoices electronically on a monthly basis. For services, invoices should include the contract line item number, item description, and period of performance and associated costs. Each page must be clearly marked with information identifying it with the company, the contract, the invoice, and any other information required by the contract.

SEC Non-Disclosure Requirements and Agreements. Non-disclosure agreements (NDA) must be completed and returned to the contracting officer before starting work under the contract. The contractor shall submit to the contracting officer a list of its employees, agents, and subcontractors that will be authorized access to SEC information. Each person identified shall sign an NDA on behalf of themselves and submit it to the contracting officer before commencing work on the contract.

Personally Identifiable Information (PII). A contractor that designs, develops, or operates a system of records on individuals, or otherwise collects or has access to PII[10] in the performance of the contract shall, prior to taking such action, comply with specific requirements. Such requirements include, but are not limited to, having policies and procedures to safeguard SEC PII; providing quarterly assessments to the SEC demonstrating that the controls for safeguarding SEC PII are functional and effective; and providing a copy of the contractor's privacy policies to the contracting officer.

Objectives

Our overall objective was to assess ENF's use of external experts between April 1, 2015, and March 31, 2017. Specifically, we sought to determine whether the SEC had implemented effective controls for:

(1) reviewing and approving requests for ENF's external experts, and for selecting individual external experts, including but not limited to conducting cost-benefit and conflict of interest analyses, evaluating the technical approach, assessing the expertise of SEC employees, performing market research, and completing other pre-award requirements when contracting with external experts; and

(2) managing its contracts with experts and the funds spent on external experts' services, fees, and expenses, as appropriate.

[10] Office of Management and Budget M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, defines PII as, "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

To address our audit objectives, we interviewed ENF and OA officials and reviewed (1) ENF's policies and procedures for retaining expert services; (2) SEC financial data for amounts obligated for and spent on expert services during our scope period; and (3) Federal laws and regulations and SEC policies and procedures for CORs and T&M/LH and other-than-full-and-open-competition contracts. We also judgmentally selected and reviewed 21 contracts for expert services awarded during our scope period, including at least 1 contract for expert services managed by each of the SEC's 11 regional offices, as well as Headquarters. For each contract selected, we reviewed COR files, official contract files, and related documentation.

Appendix I includes additional information about our objectives, scope, and methodology, including sampling; our review of internal controls; and prior coverage.

Results

Finding 1: CORs' Ability to Conduct Surveillance of Contractors' Performance Was Limited

According to SECR 10-17, "A T&M/LH contract provides no positive profit incentive to the contractor for cost control or labor efficiency; therefore, the COR must conduct appropriate surveillance of contractor performance to give reasonable assurance that the contractor is using efficient methods and effective cost controls." To help the agency conduct surveillance, the SEC required experts to submit monthly status reports. Experts generally did not submit the reports, and agency personnel did not enforce the requirement to do so. In addition, some experts submitted invoices with little or no detail about the work performed and the personnel who performed it. We identified invoices that (1) did not identify labor categories or rates charged, (2) billed for labor categories or labor rates that were not approved by the corresponding contract, and (3) resulted in the SEC being over-billed, albeit by small amounts. Because CORs for the contracts we reviewed had limited first-hand knowledge of the sufficiency of contract deliverables and work performed, they were unable to determine whether invoices accurately reflected work performed. Instead, CORs relied on ENF attorneys to determine whether invoices accurately reflected work performed. As a result, CORs' ability to conduct surveillance of contractors' performance was limited.

Experts Did Not Submit Monthly Status Reports

Although contracts for expert services generally required experts to submit to the SEC monthly status reports of all work performed under the contract, we found that this occurred for only 2 of the 21 contracts we reviewed. For the remaining 19 contracts, we determined that contract files and COR files did not include contractors' monthly status reports, and we confirmed with CORs, ENF attorneys, and other contract points-of-contact that they did not receive monthly status reports.

According to SECR 10-17, a COR should develop a surveillance plan for all T&M/LH contracts above the simplified acquisition threshold ($150,000). SECR 10-17 further states that the level and detail of the surveillance plan will depend on the contract value, criticality of services, and complexity of the contract; yet, to be effective, "contract surveillance must be timely, organized, and well documented." Although most of the expert services contracts awarded during our scope period were under the simplified acquisition threshold, we noted in several *Determination and Findings For*

Contract Type[11] the following language regarding how the SEC planned to manage and mitigate the risks associated with T&M/LH contracts: "The [COR] will manage and mitigate risks through the surveillance of the monthly status report required as a deliverable under the contract award."

We interviewed CORs and ENF attorneys associated with the 21 contracts we reviewed and determined that agency personnel did not enforce this contract requirement. Most CORs believed that ENF attorneys received monthly status reports given that the attorneys worked closely with the experts and were responsible for inspecting and accepting experts' services. However, ENF attorneys either interpreted the status report requirement loosely or did not believe receiving monthly status reports was in the best interest of the SEC. For half of the 21 contracts we reviewed, ENF attorneys stated that they maintained continuous communication with experts and, therefore, obtained status orally rather than from a formal report. ENF attorneys associated with 7 of the 21 contracts we reviewed told us that experts' invoices met the intent of the monthly status report. Moreover, four ENF attorneys we interviewed stated that SEC contracts should not require experts to submit monthly status reports because of potential litigation risk.[12]

Without receiving monthly status reports as envisioned in the contracts we reviewed, the CORs' ability to conduct surveillance of contractors' performance was limited. Moreover, as described below, CORs relied on ENF attorneys to approve invoices.

During our audit, OA personnel developed language outlining administrative requirements and adherence to contract terms and conditions of contracts for expert services. OA personnel stated that they would provide this language to experts at the commencement of each new contract for expert services. In addition, ENF and OA have been discussing eliminating the contract requirement for monthly status reports.

CORs Relied on ENF Attorneys To Approve Invoices

CORs must ensure that products or services being invoiced have been received by the SEC and meet contract requirements or standards. CORs are to approve invoices only after the delivery or performance is satisfactorily completed. A COR's approval of an invoice indicates acceptance and that the invoice conforms to the terms of the contract.

CORs told us that when they received invoices, they generally reviewed them for labor categories, labor rates, and contract periods of performance. However, because they did not communicate with experts regularly and did not inspect and accept contract deliverables, CORs stated that they relied on ENF attorneys to determine whether the

[11] The purpose of the *Determination and Findings For Contract Type* is to document the authority to enter into a T&M/LH contract for expert services.

[12] According to ENF management, a status report from an expert could become subject to discovery insofar as it relates to the expert's scope of work and compensation.

work described on the invoice was commensurate with what the expert had accomplished during the billing period. Our review of invoices revealed that the information and level of detail included in invoices varied from expert to expert. For example, some invoices provided the amount of time specific contract personnel spent on individual tasks. Other invoices simply listed individuals and the aggregate number of hours worked during the period without explaining each person's tasks. As a result, CORs with limited knowledge of the sufficiency of contract deliverables or the work performed relied on ENF attorneys for invoice approval.

For each of the 21 contracts we reviewed, we analyzed all invoices submitted by experts and paid by the SEC as of November 2017 (for a total of 120 invoices). Although we did not identify fraud, waste, or significant mismanagement of the funds spent on the experts' services, fees, and expenses we reviewed, we identified the following issues:

- For one contract awarded in September 2016, the expert had submitted and been paid for only one invoice as of November 2017 (totaling $8,996). Although contractors are required to submit invoices on a monthly basis, the billing period covered almost 3 months of work and the invoice did not include labor categories, labor rates, or the number of hours worked daily or in aggregate.[13]

- For another contract, the expert submitted an invoice totaling $128,794 that billed for six different labor categories although there was only one labor category approved in the contract (Expert at the rate of $585 per hour). Of the total amount invoiced, $27,267 (or about 21 percent) was attributable to the five labor categories not approved in the contract. We noted that OA modified the contract in March 2017 to include these labor categories.

- For another contract, the billing rate for one individual did not align with the contract terms. Specifically, a quality control partner billed at a rate of $450 per hour rather than the contract-approved rate of $390 per hour. The contractor billed for the quality control partner at this increased, unapproved rate in three different invoices for a total of 8 hours, which resulted in the contractor over-billing the SEC by $480.[14]

- For another contract, we identified two potential labor categories listed on invoices that were not approved in the contract. First, an individual listed as an intern billed 1.5 hours at a rate of $75 per hour (for a total of $112.50). Second, a "team" billed 20.8 hours at a rate of $255 per hour (for a total of $5,304). The ENF attorney who worked with this expert was not aware that the "team" was not

[13] The contract allowed for four different labor categories with labor rates ranging from $90 per hour to $406 per hour.

[14] The SEC was not aware of this issue before our audit. To resolve this issue, the SEC retroactively adjusted the hourly rate in the contract's close-out modification.

an approved labor category in the contract. However, the ENF attorney had knowledge of the work performed by the team and, therefore, approved the invoice because it was commensurate with the work the contractor performed.

- For another contract, we identified three different computational invoice errors that all resulted in the contractor over-billing the SEC. First, the contractor submitted an invoice for $98,884.75 instead of the correct amount of $98,652.25. Second, the contractor submitted an invoice for $38,613.25 instead of the correct amount of $38,602.50. Third, one of the contractor's invoices listed an expert's rate as $625 per hour rather than the contract-approved rate of $610 per hour. In total, these errors resulted in the firm over-billing the SEC by $273.25.[15]

Although we identified only small amounts over-billed to the SEC, these issues occurred because of inadequate contract management. Overall, the SEC can better manage ENF's contracts for expert services and improve the ability of agency personnel to conduct surveillance of contractors' performance. During our audit, OA began developing a supplemental invoice template to capture more consistent information related to the work experts perform and invoice.

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

To improve CORs' oversight of contractor performance under contracts for expert services, we recommend that OA work with ENF to:

Recommendation 1: Determine if surveillance of experts' monthly status reports is the optimal process for managing and mitigating contract-related risks; and, as needed, establish new processes and guidance to define the role of contracting officers' representatives in surveilling work performed under contracts for expert services.

Management's Response. Management concurred. The Office of Acquisitions will work with the Division of Enforcement to determine if surveillance of experts' monthly status reports is the optimal process for managing and mitigating contract-related risks; and, as needed, establish new processes and guidance to define the role of contracting officers' representatives in surveilling work performed under contracts for expert services. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

[15] The SEC was not aware of these issues before our audit. Because this contract has been closed, OA personnel stated that they would draft a debt letter to the firm requesting it return the overpayment amount.

Recommendation 2. Finalize the supplemental invoice template to clearly define and communicate types of information required in experts' monthly invoices submitted for payment.

Management's Response: Management concurred. The Office of Acquisitions will work with the Division of Enforcement to finalize the supplemental invoice template to clearly define and communicate types of information required in experts' monthly invoices submitted for payment. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 2: The SEC Did Not Always Enforce or Establish Information Security Controls to Address Risks Inherent in Contracts for Expert Services

ENF work may involve sensitive, non-public information that is personally identifiable, commercially valuable, and market-sensitive. The SEC must ensure that experts retained under contract who have access to such information properly safeguard it. Although the SEC established some requirements in recognition of certain information security risks, ENF and OA personnel did not always enforce those requirements. For example, agency personnel did not ensure that more than half of the 113 individuals reported as having worked on the contracts we reviewed signed the required NDA or signed one timely. In addition, in at least five instances, agency personnel had not enforced contract requirements related to PII even though experts had access to PII. We also found that contracts lacked controls regarding the inadvertent release or disclosure of information after the SEC transmits information to experts. As a result, the agency lacked assurance that experts and their information systems achieved basic levels of security to protect the SEC's sensitive, non-public information, including PII. We did not identify instances in which unauthorized individuals accessed such information after it was provided to experts. However, the agency should take steps to minimize the risk of unauthorized disclosure, modification, and use of its sensitive, non-public information provided to experts.

Contractors Did Not Always Sign or Timely Sign NDAs

SEC Operating Procedure 10-22, *Onboarding, Tracking, and Offboarding of Contractor Personnel* (Rev. 4; May 25, 2017),[16] describes NDA distribution, collection, and filing requirements and related contracting officer and COR responsibilities. The procedure states that the contractor and each of the contractor personnel (CP) must complete and sign an NDA for each contract on which CP work. For new contracts, the contracting officer provides the contractor with NDA forms and collects and files signed entity NDA forms, while the COR collects and files signed CP NDA forms. If CP join an existing contract, the COR is responsible for providing, collecting, and filing NDAs. Generally, the SEC's contracts for expert services required CP to complete and return to the contracting officer an NDA before beginning work. Moreover, the contracts generally stated that a violation of an NDA or assignment of staff who had not executed an NDA may result in administrative contracting officer action, default of the contract, civil suits,

[16] Although the SEC released Revision 4 and Revision 3 (released September 23, 2016) of this operating procedure after the commencement of the audit period (April 1, 2015), we confirmed that, with regard to NDA requirements, Revision 4, Revision 3, and Revision 2 (released August 1, 2014) were substantially the same.

or criminal prosecution. The SEC appeared to place significant reliance on experts' completion and filing of NDAs as a key information security control.

A total of 113 individuals were listed on contractor-submitted invoices as having worked on the 21 contracts we reviewed. However, 61 of these individuals, or more than half, either had not signed an NDA or signed one *after* beginning work under the contract. Specifically, as shown in Table 2, 40 of the 113 individuals (or about 35 percent) had not signed an NDA. In fact, files for 10 of the 21 contracts we reviewed were missing at least 1 NDA, including 2 contract files that were missing NDAs for all individuals who performed work under the contracts. (See Sample No. 10 and Sample No. 19 in Table 2.) In addition, of the 73 individuals who signed an NDA, 21 (or about 29 percent) signed an NDA late (that is, after beginning work). Although some of these 21 individuals signed an NDA within days of beginning work, other individuals signed an NDA much later. For example, 11 of the 12 NDAs on file for 1 contract we reviewed were signed, on average, 305 days after the individuals' names first appeared on an invoice submitted to the SEC. The remaining six individuals who performed work under the contract had not signed an NDA. (See Sample No. 13 in Table 2.) These deviations from SEC policy and established contract requirements resulted from insufficient contract oversight.

Table 2. Analysis of Individuals Who Performed Contracted Work and Signed NDAs

Sample No.	No. of Individuals Who Performed Work	No. of NDAs Signed	No. of NDAs Missing	For NDAs Signed, No. Signed Late
1	1	1	0	0
2	3	3	0	1
3	3	3	0	0
4	9	7	2	0
5	2	1	1	0
6	6	5	1	4
7	1	1	0	0
8	1	1	0	0
9	10	3	7	0
10	2	0	2	0
11	9	9	0	4
12	11	11	0	1
13	18	12	6	11
14	15	6	9	0
15	1	1	0	0
16	3	2	1	0
17	1	1	0	0
18	6	1	5	0
19	6	0	6	0
20	1	1	0	0
21	4	4	0	0
TOTAL	**113**	**73**	**40**	**21**

Source: OIG analysis of contractors' invoices and NDAs.

NDAs specifically require CP to acknowledge and honor prohibitions against the improper use and unauthorized disclosure of confidential or non-public information. If a CP discloses confidential or non-public information in violation of an NDA, the CP could be subject to administrative, civil, or criminal action. Additionally, if a CP violates the NDA, the SEC could terminate the contract and/or seek to have CP suspended or debarred from future federal contracts. The SEC's available remedies are potentially more limited for a CP who did not sign an NDA.

During our audit, OA began developing a supplemental invoice template that requires experts to confirm whether each person listed on the invoice has completed an NDA.

OA Did Not Enforce Requirements Related to PII

As previously stated, the SEC's contracts for expert services generally required contractors that collect or otherwise have access to PII in the performance of the contract to meet certain requirements before obtaining access to SEC PII. Specifically, the contractors must:

1. Have established policies and procedures in place to safeguard SEC PII.

2. Ensure that all processes, procedures, and equipment associated with PII comply with all laws, regulations, and security mandates as defined by National Institute of Standards and Technology, as well as U.S. Government and SEC policies developed to safeguard SEC data that may contain PII.

3. Provide quarterly assessments to the SEC demonstrating that the required policies, procedures, and mechanisms continue to function; that the contractor is compliant with these requirements; and that these requirements are effective.

4. Provide a copy of their privacy policies to the contracting officer. The contractor shall also provide a copy of the policies and procedures to all of its employees, agents, and subcontractors assigned to perform the requirements of the contract.

5. Ensure that the contractor's employees, agents, and subcontractors assigned to perform the requirements of the contract adhere to the contractor policies and procedures relating to PII and to SEC-prescribed policies and procedures for the safe handling of SEC PII.

6. Immediately alert the SEC of any event, including the suspected or confirmed loss of SEC PII that could potentially affect the privacy rights of individuals.

We did not obtain information ENF attorneys sent to experts. However, we asked ENF attorneys whether they had sent PII to experts. At least five attorneys stated that they had sent PII to experts. The PII included investors' names, addresses, dates of birth, and customer account information. In all five instances, prior to our audit, the contracting officer had not obtained from experts the required quarterly assessments or privacy policies.

According to the contracting officer, experts were to provide all contract deliverables to the cognizant ENF attorney. We noted that this statement was inconsistent with the contracts, which stated that experts were to provide quarterly assessments and privacy policies to the contracting officer. In addition, we noted that contracts for expert services stated that, at the time of contract formation, it was not contemplated that the contractors would be exposed to, provided with, or given access to PII. Because ENF attorneys, and not contracting officers, primarily work with experts, contracting officers were not aware of experts' access to PII. If the SEC does not enforce contract requirements related to PII when experts are given access to PII, the SEC cannot ensure that experts have policies, procedures, and mechanisms in place to safeguard SEC PII.

Contracts Lacked Controls Regarding Inadvertent Release or Disclosure of Information Provided to Experts

OA incorporated into the expert contracts we reviewed the following requirements addressing the unauthorized disclosure, use, or duplication of information:

- SEC 6001.00, *SEC Non-Disclosure Requirements and Agreements*. As previously discussed, contractor personnel must complete NDAs before beginning work, and are prohibited from unauthorized disclosure and improper use of confidential or non-public information or documents.

- SEC 6001.01, *Restrictions on Use, Disclosure, and Duplication of Confidential and Non-Public Information.* Contractors and their employees, agents, subcontractors, and subcontractor personnel cannot duplicate or disclose confidential or non-public information in whole or in part, outside the SEC for purposes other than fulfillment of contract requirements.

- SEC 6012.00, *Security and Privacy Act Matters.* Documents that shall be reviewed and produced in connection with the contract are non-public and sensitive in nature and shall be protected from unauthorized disclosure.

- SEC 6017.00, *Communicating Non-Public or Sensitive Information*. Contractors must encrypt e-mails that discuss non-public or sensitive information.

Although these requirements play an important role in safeguarding SEC information provided to experts, these requirements do not address risks posed by the unique circumstances under which experts work. For example, experts generally work remotely and are not provided SEC information technology resources or given access to the agency's network. Instead, ENF attorneys send information to experts via e-mail, discs, or external hard-drives, and experts use their own information technology resources (that is, computers, servers, networks, and software) to perform work. As a result, the information technology resources experts use are not protected by the SEC's

information security program, which protects the agency from risks of unauthorized disclosure, modification, use, and disruption of sensitive, non-public information.[17]

Federal Acquisition Regulation (FAR) 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, focuses on ensuring a basic level of safeguarding for any contractor system with Federal information.[18] Specifically, FAR 52.204-21 is a contract clause that requires, at a minimum, implementation of 15 security controls, requiring contractors to: (1) limit information system access to authorized users or devices; (2) sanitize or destroy information system media containing Federal contract information before disposal or release for reuse; and (3) update malicious code protection mechanisms when new releases are available.

When asked about FAR 52.204-21, OA personnel noted that the clause was not made effective until June 15, 2016. However, the SEC awarded 9 of the 21 contracts we reviewed (or about 43 percent) after June 15, 2016, and none of those 9 contracts included FAR 52.204-21. Although OA personnel conducted a quarterly review of contract files, that review did not include a review of new or recent FAR parts, subparts, or sections applicable to new solicitations, contracts, and modifications to existing contracts. In January 2018, during our audit, an official from the OA Office of the Director indicated that OA had begun to incorporate FAR 52.204-21 in all new solicitations, contracts, and modifications to active ENF contracts, including contracts for expert services. In addition, during our audit, OA updated its template for contracts with experts to include FAR 52.204-21 and provided us evidence that contracts issued in early 2018 included the clause.

We did not identify instances in which unauthorized individuals accessed the SEC's sensitive, non-public information provided to experts. However, at a minimum, including FAR 52.204-21 in contracts for expert services will help provide assurance that experts' information systems achieve basic levels of security to protect SEC information, including PII, and minimize the risk of unauthorized disclosure, modification, and use of such information.

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

To improve the SEC's ability to address information security risks inherent in ENF's contracts for expert services, we recommend that OA:

[17] The Federal Information Security Modernization Acts of 2014 and 2002 (Public Laws 113-283 and 107-347) require agencies to develop, document, and implement an agency-wide information security program to provide information security for the data and information systems that support the operations and assets of the agency.

[18] FAR 52.204-21 defines a "covered contractor information system" as, "…an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information." In our opinion, experts use covered contractor information systems to perform work.

Recommendation 3: Work with the Division of Enforcement to obtain non-disclosure agreements from any contractor personnel who are assigned to an active expert service contract but have not completed a non-disclosure agreement.

Management's Response. Management concurred. The Office of Acquisitions will work with the Division of Enforcement to obtain non-disclosure agreements from applicable contractor personnel who are assigned to an active expert service contract but have not completed a non-disclosure agreement. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 4: Work with the Division of Enforcement to implement a standardized process for verifying receipt of non-disclosure agreements, where necessary, and before contractor personnel perform work under any new contracts for expert services.

Management's Response. Management concurred. The Office of Acquisitions will work with the Division of Enforcement to implement a standardized process for verifying receipt of non-disclosure agreements, where necessary, and before contractor personnel perform work under any new contracts for expert services. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 5: Incorporate into the Office of Acquisition's processes a review of new or recent Federal Acquisition Regulation parts, subparts, or sections applicable to new solicitations, contracts, and modifications to existing contracts, including Federal Acquisition Regulation 52.204-21.

Management's Response. Management concurred. The Office of Acquisitions will incorporate into its processes a review of new or recent Federal Acquisition Regulation parts, subparts, or sections applicable to new solicitations, contracts, and modifications to existing contracts, including Federal Acquisition Regulation 52.204-21. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 6: Work with the Division of Enforcement to (a) determine if the current contractual provisions regarding protection of personally identifiable information are the optimal processes for ensuring appropriate protection of such information, and

(b) evaluate what other steps are needed to ensure contractors appropriately protect such information.

Management's Response. Management concurred. The Office of Acquisitions will work with the Division of Enforcement to (a) determine if the current contractual provisions regarding protection of personally identifiable information are the optimal processes for ensuring appropriate protection of such information, and (b) evaluate what other steps are needed to ensure contractors appropriately protect such information. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 7: Work with the Division of Enforcement to develop a process that ensures contracting officers enforce contract requirements related to personally identifiable information, when necessary, for any new contracts for expert services.

Management's Response. Management concurred. The Office of Acquisitions will work with the Division of Enforcement to develop a process that ensures contracting officers enforce contract requirements related to personally identifiable information, when necessary, for any new contracts for expert services. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Appendix I. Scope and Methodology

We conducted this performance audit from June 2017 through June 2018 in accordance with generally accepted government auditing standards. 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.

Scope. The audit covered contracts for expert services awarded between April 1, 2015, and March 31, 2017. Our objective was to assess ENF's use of external experts. Specifically, we sought to determine whether the SEC had implemented effective controls for:

(1) reviewing and approving requests for ENF's external experts, and for selecting individual external experts, including but not limited to conducting cost-benefit and conflict of interest analyses, evaluating the technical approach, assessing the expertise of SEC employees, performing market research, and completing other pre-award requirements when contracting with external experts; and

(2) managing its contracts with experts and the funds spent on external experts' services, fees, and expenses, as appropriate.

We performed fieldwork at the SEC's Headquarters in Washington, DC, although we assessed contracts for expert services managed by each of the SEC's 11 regional offices, as well as Headquarters.

Methodology. We interviewed ENF officials to understand the SEC's policies and procedures for retaining experts and managing contracts for expert services. We also interviewed OA officials to understand the agency's policies and procedures for awarding contracts that are other than full and open competition. In addition, we reviewed SEC financial data for amounts obligated for and spent on expert services during our scope period, Federal laws and regulations and SEC policies and procedures for other-than-full-and-open-competition contracts, and official contract files and related documentation for 21[19] judgmentally selected contracts for expert services.

We limited our sample size to 21 of the 197 contracts equal to or greater than $1,000 awarded during our scope period (or about 11 percent). The number of contracts

[19] Initially, we judgmentally selected 22 contracts for expert services. We then learned that one expert did not perform any work and OA closed the corresponding contract. Although we could assess the selection and hiring of the expert, we could not test for compliance with contract requirements, including invoicing and submission of an NDA. As a result, we reported on the results of our review of the other 21 contracts in our sample.

selected from each SEC regional office was representative of each office's relationship to the whole population. The sample included at least one contract from each SEC regional office and a variety of contracts that fell within established dollar value thresholds (that is, below $150,000; between $150,000 and $700,000; and more than $700,000). Because sampled items were non-statistical, we did not project our results and conclusions to the total population of contracts for expert services.

Internal Controls. To assess internal controls related to our objectives, we reviewed ENF's management assurance statements and risk assessments for fiscal years 2015 and 2016. ENF management reported that it tested control activities to evaluate the design and effectiveness of internal controls. Moreover, management acknowledged that ENF (1) could better secure and protect PII in accordance with the Privacy Act, and (2) is considering process improvements to tighten the security and protection of PII and to coordinate with other SEC divisions and offices regarding system security and best practices. However, ENF management also reported that none of the issues or challenges management identified rose to the level of a material weakness or created the risk of a material weakness. As a result, ENF management concluded that the controls and processes in place were effective.

We also tested key internal controls related to ENF's selection of experts and management of expert contracts. Specifically, we assessed (1) ENF attorneys' process for performing market research and selecting experts, (2) ENF management's review and approval process, and (3) CORs' process for reviewing and approving invoices. To do so, we reviewed a non-statistical sample of 21 judgmentally selected contracts awarded during the period of scope, including supporting documentation such as expert request forms, internal correspondence, contract modifications, invoices, NDAs, and other documents related to contract award. We determined that the internal controls ENF implemented for reviewing and approving requests and for selecting experts were operating effectively. However, as discussed in this report, we identified internal control weaknesses that affected the SEC's ability to ensure that (1) contracts for expert services are properly managed; and (2) sensitive, non-public information provided to experts is protected from inadvertent release, disclosure, or unauthorized access. Our recommendations, if implemented, should correct the weaknesses we identified.

Computer-processed Data. We did not rely significantly on computer-processed data to address our audit objectives. Therefore, we did not assess any system controls or the reliability of any computer-processed data.

Prior Coverage. Between 2013 and 2017, the SEC OIG and the Government Accountability Office issued the following reports of particular relevance to this audit:

SEC OIG:

- *Audit of SEC's Controls over Support Service, Expert and Consulting Service Contracts* (Audit Report No. 513, March 29, 2013).

Government Accountability Office:

- *Service Contracts, Agencies Should Take Steps to More Effectively Use Independent Government Cost Estimates* (GAO-17-398, May 2017).

These reports can be accessed at: https://www.sec.gov/oig (SEC OIG) and https://www.gao.gov/ (Government Accountability Office).

Appendix II. Management's Comments

MEMORANDUM FOR REBECCA SHAREK, DEPUTY INSPECTOR GENERAL FOR AUDITS, EVALUATIONS, AND SPECIAL PROJECTS

FROM: Kenneth A. Johnson
Chief Operating Officer

DATE: June 7, 2018

SUBJECT: Response to Draft Report on SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement

Thank you for the opportunity to review and comment on the draft report on the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement.

We appreciate your acknowledgment of the corrective actions we have already taken to strengthen our internal controls associated with retaining external experts and foreign counsel. We welcome your recommendations on how we can further improve. As we note below, we concur with the recommendations in your draft report. We believe they correctly identify opportunities to continue to improve our processes and procedures to help contracting officer representatives more effectively monitor work performed under contracts for expert services, ensure contracting officers enforce contract requirements related to personally identifiable information, and establish standard verification of non-disclosure agreement receipt for individuals that work under contracts for expert services. A response to each of the recommendations is provided below.

Recommendation 1: Determine if surveillance of experts' monthly status reports is the optimal process for managing and mitigating contract-related risks; and, as needed, establish new processes and guidance to define the role of contracting officers' representatives in surveilling work performed under contracts for expert services.

Management Response: Management concurs. The Office of Acquisitions will work with the Division of Enforcement to determine if surveillance of experts' monthly status reports is the optimal process for managing and mitigating contract-related risks; and, as needed, establish new processes and guidance to define the role of contracting officers' representatives in surveilling work performed under contracts for expert services.

Recommendation 2: Finalize the supplemental invoice template to clearly define and communicate types of information required in experts' monthly invoices submitted for payment.

Management Response: Management concurs. OA will work with ENF to finalize the supplemental invoice template to clearly define and communicate types of information required in experts' monthly invoices submitted for payment.

Recommendation 3: Work with the Division of Enforcement to obtain non-disclosure agreements from any contractor personnel who are assigned to an active expert service contract but have not completed a non-disclosure agreement.

Management Response: Management concurs. OA will work with ENF to obtain non-disclosure agreements from applicable contractor personnel who are assigned to an active expert service contract but have not completed a non-disclosure agreement.

Recommendation 4: Work with the Division of Enforcement to implement a standardized process for verifying receipt of non-disclosure agreements, where necessary, and before contractor personnel perform work under any new contracts for expert services.

Management Response: Management concurs. OA will work with ENF to implement a standardized process for verifying receipt of non-disclosure agreements, where necessary, and before contractor personnel perform work under any new contracts for expert services.

Recommendation 5: Incorporate into the Office of Acquisition's processes a review of new or recent Federal Acquisition Regulation parts, subparts, or sections applicable to new solicitations, contracts, and modifications to existing contracts, including Federal Acquisition Regulation 52.204-21.

Management Response: Management concurs. OA will incorporate into its processes a review of new or recent Federal Acquisition Regulation parts, subparts, or sections applicable to new solicitations, contracts, and modifications to existing contracts, including Federal Acquisition Regulation 52.204-21.

Recommendation 6: Work with the Division of Enforcement to (a) determine if the current contractual provisions regarding protection of personally identifiable information are the optimal processes for ensuring appropriate protection of such information, and (b) evaluate what other steps are needed to ensure contractors appropriately protect such information.

Management Response: Management concurs. OA will work with ENF to (a) determine if the current contractual provisions regarding protection of personally identifiable information are the optimal processes for ensuring appropriate protection of such information, and (b) evaluate what other steps are needed to ensure contractors appropriately protect such information.

Recommendation 7: Work with the Division of Enforcement to develop a process that ensures contracting officers enforce contract requirements related to personally identifiable information, when necessary, for any new contracts for expert services.

Management Response: Management concurs. OA will work with ENF to develop a process that ensures contracting officers enforce contract requirements related to personally identifiable information, when necessary, for any new contracts for expert services.

Finally, we would like to express our appreciation for the courtesy you and your staff extended to us during this audit. If you have any questions or would like to discuss any of our comments, please let us know.

cc: Stephanie Avakian, Co-Director, Division of Enforcement
Steven Peikin, Co-Director, Division of Enforcement
Vance Cathell, Director, Office of Acquisitions
David Gottesman, Deputy Chief Litigation Counsel, Division of Enforcement
Wanda Armwood, Assistant Director, Contract Planning & Oversight, Division of Enforcement
Margaret McGuire, Senior Counsel to the Co-Directors, Division of Enforcement

2

Major Contributors to the Report

Colin Heffernan, Audit Manager

Juan Figueroa, Lead Auditor

Michael Gainous, Auditor

Matthew Fryer, Auditor

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

Web: https://www.sec.gov/oig

Fax: (202) 772-9265

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

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments 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.