U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Operating efficiently and effectively

EPA Budget Systems Need Improved Oversight of Security Controls Testing

Report No. 20-P-0015 **November 1, 2019**

Report Contributors: Rudolph M. Brevard
Albert E. Schmidt
Teresa L. Richardson

Abbreviations

BAS	Budget Automation System
BFS	Budget Formulation System
EPA	U.S. Environmental Protection Agency
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
SAR	Security Assessment Report

Cover Image: Security controls testing is a critical element that facilitates the security of the EPA's budget systems. (OIG image)

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

20-P-0015
November 1, 2019

At a Glance

Why We Did This Project

The Office of Inspector General (OIG) conducted this audit to determine whether the Office of the Chief Financial Officer (OCFO) identified and tested all required security controls for the U.S. Environmental Protection Agency's (EPA's) legacy budget system—called the Budget Automation System (BAS). We also sought to determine whether the EPA required the cloud service provider for the agency's replacement budget system—called the Budget Formulation System (BFS)—to comply with National Institute of Standards and Technology requirements for testing information system security controls.

The OCFO's Office of Budget is responsible for the BAS and BFS. The OCFO relies on service providers to support and host the systems. An EPA data center hosts the BAS, while a contractor hosts the BFS in a cloud environment. Various entities within and outside the EPA provide security controls for the BAS and BFS.

This report addresses the following:

- *Operating efficiently and effectively.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

List of OIG reports.

EPA Budget Systems Need Improved Oversight of Security Controls Testing

What We Found

The OCFO identified the required security controls needed for the agency's budget systems.

For the BAS, the OCFO and its service providers tested 100 percent of the security controls in our fiscal year 2016 sample. However, the OCFO and its service providers did not test all of the security controls in our fiscal year 2017 sample.

The OCFO lacks internal controls needed to make informed, risk-based decisions regarding the security of the agency's budget systems.

For the BFS, the OCFO required the cloud service provider to comply with National Institute of Standards and Technology testing requirements. However, the OCFO did not maintain documentation to substantiate whether (1) the BFS cloud service provider tested and implemented the required security controls or (2) the controls were working as intended to protect the BFS and its data.

Additionally, we found that the OCFO:

- Did not correctly assign and document responsibility for testing BAS security controls.
- Did not review BFS security reports in a timely manner or document the results of these reviews.

Testing security controls enables organizations to identify vulnerabilities in their systems. Finding these vulnerabilities in a timely manner would allow the EPA to promptly remediate any weaknesses that impact the safety of its systems. Likewise, a lack of internal controls means vulnerabilities are found late or not at all, and prevents the EPA from protecting its budget data from unauthorized disclosures or modifications.

Recommendations and Planned Agency Corrective Actions

We recommend that the Chief Financial Officer update the BAS security planning documents to specify who is responsible for testing information system security controls, as required by the National Institute of Standards and Technology. We also recommend that the Chief Financial Officer implement a process for obtaining and documenting the timely review of all BAS and BFS security reports.

The EPA agreed with our recommendations. The agency provided sufficient evidence that it completed corrective actions for Recommendation 1 and the recommendation is resolved. The agency did not provide a milestone date or acceptable documentation to support that it completed corrective actions for Recommendation 2, and that recommendation is, thus, unresolved.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

November 1, 2019

MEMORANDUM

SUBJECT: EPA Budget Systems Need Improved Oversight of Security Controls Testing
Report No. 20-P-0015

FROM: Charles J. Sheehan, Acting Inspector General

TO: David Bloom, Acting Chief Financial Officer

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY18-0065. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determination on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The EPA's Office of the Chief Financial Officer and its Office of Budget are responsible for the issues discussed in this report.

Action Required

We made two recommendations in this report. In accordance with EPA Manual 2750, your office completed acceptable corrective actions in response to Recommendation 1. Recommendation 1 is resolved, and no final response to Recommendation 1 is required.

For Recommendation 2, your office did not provide us a milestone date or evidence to support the completion of the corrective actions. Therefore, Recommendation 2 is unresolved. In accordance with EPA Manual 2750, you are required to provide a written response to this report within 60 calendar days. You should include planned corrective actions and completion dates for Recommendation 2 for resolution.

Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. Your response will be posted on the OIG's website, along with our memorandum commenting on your response. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Purpose 1

Background 1

Responsible Offices 2

Scope and Methodology 2

Results 3

Not All BAS Security Controls Were Tested 4
OCFO Did Not Review BFS SAR in a Timely Manner and Did Not Maintain Documentation of Its Review 4

Conclusion 5

Recommendations 6

EPA Response and OIG Evaluation 6

Status of Recommendations and Potential Monetary Benefits 7

Appendices

A **EPA Response to Draft Report** 8

B **Distribution** 11

Purpose

The Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) conducted this audit to determine whether the Office of the Chief Financial Officer (OCFO) identified and tested all information system security controls as required by the National Institute of Standards and Technology (NIST). Specifically, we sought to determine whether the OCFO identified and tested all inherited security controls for the EPA's legacy Budget Automation System (BAS) and required that the contractor for the replacement budget system—the Budget Formulation System (BFS)—comply with NIST requirements for testing information system security controls.

NIST defines an ***inherited security control*** as a security capability that is provided by another entity.

Background

The EPA budget systems contain confidential information. The disclosure or release of confidential budget information outside the agency is prohibited unless specifically authorized by the EPA's OCFO. Therefore, secure budget systems are essential to protecting and managing budget decisions.

The OCFO uses two centralized budget systems—the BAS and BFS—to plan, formulate and track the performance of the agency's budget. The BAS is the EPA's legacy budget system, while the BFS is a cloud-based system that the EPA began using to formulate its 2017 budget. Once fully operational, the BFS will replace the BAS. Both the BAS and BFS link budget and performance data in support of the EPA's efforts to implement the requirements of the Government Performance and Results Act. The EPA's budget personnel also use data from the systems to generate the EPA's budget submissions to Congress and the Office of Management and Budget, prepare operating plans, and monitor budget execution.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* outlines the information system security controls that must be implemented for computer systems. This NIST guidance also requires agencies to understand the security status of their systems, even if the security controls are provided by third parties.

The OCFO's Office of Budget is the BAS and BFS system owner but relies on service providers to support and host the systems. An EPA data center hosts the BAS, while a contractor (hereafter referred to as the *cloud service provider*) hosts the BFS in a cloud environment. As the systems' owner, the OCFO has purview over the BAS and BFS system-level security controls. Other EPA offices and the cloud service provider have purview over enterprise-level security controls, and the cloud

Enterprise-level security controls are those that reside apart from but still affect a system, such as physical and environmental protection security controls (e.g., keys, guards and alarms).

service provider has purview over the security controls that reside in the BFS cloud environment. The service providers submit security assessment reports (SARs) to the system owner detailing the testing of the controls under their purview.

According to NIST, identifying security controls is an organization-wide exercise that involves senior information security officers, information system owners and other organizational officials. According to the EPA's *Information Security Policy*, Directive No. CIO 2150.4, dated December 28, 2016, the Chief Information Officer is responsible for "[e]nsuring the EPA Information Security Program and protection measures are compliant with FISMA [Federal Information Security Modernization Act] and related information security directives." The BAS and BFS system owner is responsible for coordinating with others within and outside of the EPA to implement security controls. The BAS and BFS Information System Security Officer supports the system owner in implementing the EPA's security program and verifying that controls are compliant with federal and related information security directives.

Responsible Offices

As the systems' owner, the OCFO and its Office of Budget are ultimately responsible for ensuring that all BAS and BFS security controls are tested by the service provider designated in the EPA's *Information Security and Privacy Control Guide*. All control providers must follow NIST guidance when testing security controls for government systems.

The EPA's ***Information Security and Privacy Control Guide*** is a spreadsheet that defines the required security controls for EPA information systems, as well as what entities are responsible for testing these controls.

Scope and Methodology

We conducted this audit from December 2017 to June 2019 in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. 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 to date provides a reasonable basis for our findings and conclusions based on our audit objectives.

We conducted audit work at EPA headquarters in Washington, D.C. We reviewed the BAS fiscal years 2016 and 2017 SARs to determine whether the security controls in our sample were tested by either the OCFO or the service provider, as designated in the EPA's *Information Security and Privacy Control Guide*. We obtained a list of inherited security controls for the BAS, and we judgmentally selected 20 percent of the security controls identified on the list to audit.

In addition, we reviewed the BFS cloud service provider's contract to determine whether the EPA included clauses requiring the cloud service provider to comply with federal and EPA requirements for testing security controls. We reviewed the cloud service provider's June 2017 SAR to determine what security controls it tested. We interviewed OCFO personnel to determine whether they were aware of the status of the security control testing conducted by the cloud service provider.

We were unable to evaluate what steps the OCFO took to review the BFS SAR because an OCFO employee destroyed notes regarding the SAR review. We reported this impediment to EPA officials in OIG Report No. 19-N-0085, *Management Alert: Destruction of a Document Used to Certify Security of EPA's Budget Formulation System*, issued March 8, 2019. We were still able to obtain enough information to answer our objectives, although this impediment impacted our ability to determine definitively whether the OCFO reviewed the BFS SAR. However, we believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results

We found that the OCFO required, via appropriate contract clauses, the cloud service provider to comply with agency policies and procedures. The contract also specified that these policies and procedures were to be used in conjunction with NIST guidance for information system security controls. In addition, we found that the OCFO and its service providers tested 100 percent of the security controls in our fiscal year 2016 BAS sample. However, the OCFO and its service providers did not test three of the 17 security controls in our fiscal year 2017 BAS sample. Further, the OCFO could not verify that all required security controls for the BFS were fully implemented and protecting the BFS and its data.

NIST Special Publication 800-53, Revision 4, states that responsible "officials … must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that mitigate risks to an acceptable level." We found that the OCFO did not:

- Correctly designate responsibility for testing the BAS inherited security controls to follow the EPA's *Information Security and Privacy Control Guide*.

- Review the BFS SAR in a timely manner or maintain documentation of the results of the review.

The OCFO's lack of internal controls over the process for obtaining and using security data regarding the agency's budget systems inhibits the EPA's ability to make informed, risk-based decisions to protect its data from unauthorized disclosures or modifications.

Not All BAS Security Controls Were Tested

In fiscal year 2016, 100 percent of the security controls in our sample were tested. However, in fiscal year 2017, only 82 percent of the security controls in our sample were tested. Table 1 details these findings.

Table 1: BAS inherited security controls tested (by fiscal year)

	Inherited controls	
	2016	2017
Total population of security controls scheduled to be tested	103	87
Controls in OIG sample	20	17
Controls in our sample tested by the control provider	20	14
Percent tested by the control provider	100%	82%
Controls in our sample not tested by the control provider	0	3
Percent not tested by the control provider	0%	18%

Source: OIG analysis.

The OCFO and its service providers did not test three fiscal year 2017 controls because the control testing responsibilities documented in the OCFO's internal *BAS System Security Plan* differed from those documented in the EPA's *Information Security and Privacy Control Guide.* In addition, the OCFO did not follow the EPA's guidance for defining the BAS inherited security controls to be tested. As a result, some BAS security controls were not tested.

OCFO personnel told us during our audit fieldwork that the contracted BAS control assessor/tester agreed with and conducted testing in accordance with the OCFO's *BAS System Security Plan*. In the OCFO's response to our discussion document, which outlined our initial findings and which we provided to the agency on June 25, 2018, OCFO personnel agreed with our recommendation to update the *BAS System Security Plan* to specify who is responsible for testing all relevant information system security controls.

OCFO Did Not Review BFS SAR in a Timely Manner and Did Not Maintain Documentation of Its Review

The OCFO required the BFS cloud service provider to follow NIST requirements when conducting security controls assessments. The cloud service provider made the SAR available to its clients on June 12, 2017. However, the OCFO did not review the SAR until after we brought the matter to its attention on June 25, 2018. Further, the OCFO provided no evidence that allowed the OIG to evaluate whether the OCFO (1) verified that the BFS cloud service provider implemented or tested any of the required controls or (2) evaluated the impact of the vulnerabilities noted in the BFS SAR.

During a March 2019 meeting with the OIG, OCFO personnel indicated that the OCFO was waiting until the spring of 2019 to conduct a formal review of the cloud service provider's upcoming SAR, as this timing would coincide with the renewal of the BFS' authorization to operate. They also said that the OCFO conducted an "informal" review of the cloud service provider's June 2017 SAR, which consisted of making "a few checks or tick marks here and there on the spreadsheet to keep track while reviewing the controls on-line." OCFO personnel further indicated that the purpose of the informal review was to determine that all inherited controls were in place and there were no open Plans of Action and Milestones that raised the risk level to an unacceptable level. However, OCFO staff said that once this "informal" review was completed, the OCFO's Information System Security Officer destroyed the spreadsheet that contained the review notations, per the officer's understanding of the requirements of a nondisclosure agreement with the U.S. General Services Administration. As mentioned earlier in this report, we discussed this issue in OIG Report No. 19-N-0085.

An ***authorization to operate*** is an official management decision given by a senior official who accepts the risks to authorize the operation of an information system.

Subsequently, the OCFO provided the OIG with a Memorandum for Record documenting the OCFO's review of a May 2019 BFS SAR. The OCFO indicated that the Memorandum for Record would serve as an artifact that will be uploaded into the EPA's central information security repository.

The EPA's *Information Security – Security Assessment and Authorization Procedures*, Classification No. CIO 2150-P-04.2, dated May 27, 2016, requires that security assessments be performed annually. Specifically, the procedures state that the system owner is responsible for determining the extent to which security controls are implemented correctly, operating as intended and producing the desired outcome to meet the security requirements for the system. Typically, these activities are accomplished by reviewing a control provider's SAR. However, throughout our audit, EPA personnel made various statements regarding their review of the cloud service provider's SAR, but they were unable to provide documentary evidence of the actions they took to review the SAR.

Conclusion

The OCFO lacks internal controls to verify that it has all the data needed to make informed, risk-based decisions for the BAS and BFS. Without an understanding of its budget systems' security status, the OCFO cannot effectively protect its budget data from unauthorized disclosures or modifications.

Recommendations

We recommend that the Chief Financial Officer:

1. Update the Budget Automation System's security planning documents to designate responsibilities for testing information system security controls, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

2. Implement a process for obtaining and conducting the timely review of all security assessment reports for the budget system hosting environments, and document the results of these reviews.

EPA Response and OIG Evaluation

The EPA agreed with our recommendations and provided the following acceptable corrective actions:

- Recommendation 1: Updated the appropriate system security plans to identify security controls as common, system-specific or hybrid, per federal requirements. The agency also stated that it designated the position responsible for identifying, monitoring and verifying that the security controls are tested.

- Recommendation 2: Implemented a process for obtaining and conducting the timely review of all security assessment reports for the budget system hosting environment, as well as documenting the results of these reviews.

The EPA provided us the updated *BAS System Security Plan* to show the completion of corrective actions to address Recommendation 1. The EPA did not provide us with the requested milestone date or acceptable documentation to support the completion of corrective actions for Recommendation 2. The EPA directed us to review a website with policies and procedures related to reviewing security assessment reports. However, the website did not contain documents for this area. We brought this to the agency's attention and asked them for additional documentation that supports the completion of the corrective action. The agency did not provide further information. Therefore, Recommendation 2 is unresolved.

In response to our draft report, the EPA also provided editorial comments to the "Background" and "Scope and Methodology" sections of the report. We corrected the "Background" section as appropriate. We did not modify the "Scope and Methodology" section because, as noted in this report, an agency employee deleted the information requested by the OIG. We were, therefore, unable to determine whether the employee analyzed the information security reports provided by the cloud service provider. The EPA's full response to our draft report is in Appendix A.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	6	Update the Budget Automation System's security planning documents to designate responsibilities for testing information system security controls, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.	C	Chief Financial Officer	9/4/19	
2	6	Implement a process for obtaining and conducting the timely review of all security assessment reports for the budget system hosting environments, and document the results of these reviews.	U	Chief Financial Officer		

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

EPA Response to Draft Report

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

SEP 06 2019

OFFICE OF THE
CHIEF FINANCIAL OFFICER

MEMORANDUM

SUBJECT: Response to the Office of Inspector General's Draft Report: *EPA Budget Systems Need Improved System Security Control Testing,* Project No.OA-FY18-0065

FROM: David A. Bloom, Acting Chief Financial Officer

TO: Rudolph M. Brevard, Director
Information Resources Management Directorate
Office of Inspector General

Thank you for your August 7, 2019 *EPA Budget Systems Need Improved System Security Control Testing* draft report, which directs the Office of the Chief Financial Officer to resolve two corrective actions. The OCFO has reviewed the corrective actions and will take the following actions to address them. In addition, we are asking you to clarify or correct three statements in the report that appear to be in error or have the potential to cause confusion.

Corrective Action l
Update the Budget Automation System's security planning document to designate responsibilities for testing information system security controls, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4.

OCFO Response
The OCFO has updated appropriate System Security Plans to identify security controls as common, system-specific or hybrid in accordance with the NIST's Special Publication 800-53, Revision 4. Specifically, the OCFO added an additional statement in its SSPs under section CA-7, Continuous Monitoring, to specify that it is the responsibility of the Budget Automation System's Information Systems Security Officer in coordination with the OCFO's Primary Information Security Officer to identify controls as common. system-specific or hybrid and to verify that these controls are monitored and tested per NIST's Special Publication 800-53, Revision 4.

Corrective Action 2
Implement a process for obtaining and conducting the timely review of all security assessment reports for the budget system hosting environment and document the results of these reviews.

OCFO Response

OCFO has implemented a process for obtaining and conducting the timely review of all security assessment reports for the budget system hosting environment and documenting the results of these reviews. The OCFO coordinates with the U.S. Environmental Protection Agency's host providers through established processes for managing risks. Controls identified as common controls - which includes the common control providers' portions of hybrid controls - are tested by a third-party assessor and oversight by the Office of Mission Support's Office of Enterprise Information Programs, which ensures vulnerabilities discovered are appropriately mitigated. Monthly, the OCFO reviews the lnfoSec status reports and enterprise InfoSec metrics from the OMS' EIP to stay informed of lnfoSec status information. including common controls. Common control providers notify and coordinate with the OCFO when changes that affect the OCFO's systems are needed. These processes and activities provide many data points throughout the interim period between authorizations that inform the OCFO's Senior Information Official on control status as well as other issues that impact the OCFO's systems security or when considering risks for authorization decisions.

Reviewing the report, the OCFO also would like to correct the following matters:

1. Page 1 Background Section - Report states "The disclosure or release of confidential budget in fom1ation outside the agency is prohibited unless specifically authorized by the EPA's Office of the Comptroller."

   Correction: Release of confidential budget information outside of the agency is controlled by the Office of Chief Financial Officer not the Office of the Comptroller.

2. Page 3 Scope and Methodology Section - The draft report states that ·'an OCFO employee destroyed notes" regard ing system security controls.

   Correction: Per OCFO's March 22. 2019 response to the OIG's March 8, 2019 *Management Alert: Destruction of a Document Used to Certify Security of EPA 's Budget Formulation System.* OCFO employees did not improperly destroy notes, as alleged on page 3. As fully explained in OCFO's March 22, 2019 response, an OCFO staffer used the FedRAMP Control Implementation summary, a publicly available spreadsheet, to guide his pre liminary review of the secure controls in the Microsoft Azure Authorization to Operate package, which was contained in a secure, online site. As the EPA further explained in its March 22, 2019 response, the OCFO staffer did not take notes on the spreadsheet, but rather made a few checks or tick marks to keep track of which controls he had reviewed on the online site. Following FedRAMP requirements, the reviewer properly disposed of the spreadsheet. The spreadsheet was not a federal record, and the spreadsheet was disposed of in accordance with the National Archives and Records Administration's approved disposition instructions. See June 2 1, 2019 letter from Lawrence Brewer, Chief Records Officer, NARA, to John Ellis, EPA Records Officer (closing case concerning the above-referenced matter and noting that reference materials

are non-records). Accordingly, references to the OCFO destroying documents should be removed from the report. The spreadsheet was disposed of consistent with the NARA's approved disposition instructions.

3. Page 3 and 4 Results Section - Report states that for FY 2017 not all controls were tested.

   Correction: The OCFO works with the OMS to test all required controls each fiscal year, in accordance with established test plans. The OCFO requests information on which controls the Inspector General's review team believes were not tested and/or reviewed. This information will allow the OCFO to either take corrective action to ensure controls are tested/reviewed in accordance with our testing plan or improve our documentation.

If you have any questions regarding this response, please contact Ebonie Smith, Management, Integrity and Accountability Branch, Office of the Controller at (9 19) 541-4387 or Smith.Ebonie@epa.gov.
Attachments

cc: Carol Terris
Paige Hanson
Maria Williams
Beth Baden
Ruth Soward
Mike Callewaert
Diane Kelly
Jeanne Conklin
Richard Gray
Aileen Atcherson
Sherri Anthony
Ebonie Smith
Annette Morant
Donna J. Vizian
David Zeckman
Marilyn Braxton
Vaughn Noga
Jeff Wells
Sharon Gonder

Appendix B

Distribution

The Administrator
Assistant Deputy Administrator
Associate Deputy Administrator
Chief of Staff
Deputy Chief of Staff
Chief Financial Officer
Deputy Chief Financial Officer
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Director, Office of Continuous Improvement, Office of the Administrator
Controller, Office of the Controller, Office of the Chief Financial Officer
Deputy Controller, Office of the Controller, Office of the Chief Financial Officer
Director, Office of Budget, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of Budget, Office of the Chief Financial Officer