PROPOSAL TO PROVIDE
INTERNAL AUDIT CO-SOURCING SERVICES

SUBMITTED TO
GEORGE MASON UNIVERSITY

Request for Proposals: GMU-1709-21
February 24, 2021

Cotton & Company LLP
333 John Carlyle Street, Suite 500
Alexandria, Virginia 22314
703.836.6701 [voice]
703.836.0941 [fax]
www.cottoncpa.com
Contact: Megan Mesko, CPA, CFE
MMesko@cottoncpa.com

FEI/FIN Number: 54-1172176
SWaM Certification Number: 704647
DUNS Number: 101919660
[redacted]

DISCLOSURE RESTRICTION

This proposal includes data that shall not be used or disclosed outside George Mason University (Mason) and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate the proposal. If, however, a contract is awarded to the Offeror as a result of or in connection with the submission of this data, Mason shall have the right to duplicate, use, or disclose the data to the extent consistent with its needs in the procurement process, including posting successful quotes and contracts. This restriction does not limit Mason's right to use, without restriction, information contained in the data if it is obtained from another source. The data subject to this restriction include the following:

Summary of Information to Be Protected		
Information to Be Protected	**Section/Page Number**	**Why Protection Is Necessary**
Cage Code	Cover Page	Information not generally available to the public.
Partner signature	Page 2 of the cover letter and the Mason cover page on page 2 of the proposal	Sensitive information not generally available to the public.
Names of Cotton team members	Text boxes, pages 8 through 9	Names of employees not generally available to the public.
Names of proposed team members	Text boxes, pages 16 and 20	Names of employees not generally available to the public.
Past performance contract information	Section 3.a., pages 18 through 19	Contract information not generally available to the public.
Names of proposed team members	Section 4.a.6.a., pages 28 through 30	Names of employees not generally available to the public.
Past performance contract information and point of contact (POC) names and contact information	Section 4.a.8., pages 32 through 33	Contract information and names/contact information of client personnel not generally available to the public.
Names of proposed team members and license numbers	Appendix A, Personnel Resumes	Names of employees not generally available to the public. License numbers serve as identifying information for the employees.

We have highlighted this data in our proposal and have provided a separate redacted proposal document.

Cotton & Company
Answers Questioned

333 John Carlyle Street, Suite 500 | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

February 24, 2021

James F. Russell, Director
Erin Rauch, Assistant Director
Purchasing Department
4400 University Drive, Mailstop 3C5
Fairfax, VA 22030

Subject: Proposal to Provide Internal Audit Co-Sourcing Services to George Mason University

Dear Mr. Russell and Ms. Rauch,

Cotton & Company LLP is pleased to submit our proposal to provide internal audit co-sourcing services to George Mason University's (Mason's) Office of Audit, Risk and Compliance Committee. We are well qualified to provide these services, as we demonstrate in this proposal.

Cotton & Company is a veteran-owned business founded in 1981 and headquartered in Alexandria, Virginia. Since our founding, we have concentrated our practice on providing high-quality professional audit and consulting services. We have many repeat clients, which we consider evidence of our outstanding knowledge, skills, and capacity.

Our firm is well-suited to provide the requested services, having performed thousands of contract, grant, and compliance audits and reviews of Institutes of Higher Education (IHEs), as well as dozens of construction audits/reviews and information technology and cybersecurity audits. Our significant past experience performing audits and compliance reviews at IHEs will enable us to staff this engagement with experienced personnel who have the knowledge, skills, and experience necessary to perform the proposed engagements. In particular, our past experience providing co-sourcing services to various offices at Mason has provided us with highly relevant Banner experience that makes our team uniquely qualified to provide the requested services.

Cotton & Company offers directly relevant experience gained since 1981, an outstanding professional reputation, qualified personnel, and competitive rates. We welcome this opportunity to assist Mason's Office of Audit, Risk and Compliance Committee in meeting its internal audit and other compliance and process improvement related responsibilities and are available to clarify any aspect of this proposal.

Please feel free to contact me via phone at 703.836.6701 or via email at MMesko@cottoncpa.com if I can provide any additional information.

Best regards,
Cotton & Company LLP

Megan Mesko, CPA, CFE
Partner

TABLE OF CONTENTS

PROPOSAL TO PROVIDE INTERNAL AUDIT CO SOURCING SERVICES
GEORGE MASON UNIVERSITY

1. PROCEDURAL INFORMATION [RFP SECTION XIII, PARAGRAPH B.1. PROCEDURAL INFORMATION]

Cotton & Company LLP is pleased to submit our proposal to provide internal audit co-sourcing services to George Mason University (Mason). We have provided the required procedural information on the following pages.

1.A. COVER PAGE [RFP SECTION XIII, PARAGRAPH B.1.A. RETURN SIGNED COVER PAGE AND ALL ADDENDA, IF ANY, SIGNED AND COMPLETED AS REQUIRED]

We have provided our signed cover page on the following page.

Purchasing Department
4400 University Drive, Mailstop 3C5
Fairfax, VA 22030
Voice: 703.993.2580 | Fax: 703.993.2589
http://fiscal.gmu.edu/purchasing/

REQUEST FOR PROPOSALS
GMU-1709-21

ISSUE DATE:	January 29, 2021
TITLE:	Internal Audit Co Sourcing Services
PRIMARY PROCUREMENT OFFICER:	James F. Russell, Director, jrussell@gmu.edu
SECONDARY PROCUREMENT OFFICER:	Erin Rauch, Assistant Director, erauch@gmu.edu

QUESTIONS/INQUIRIES: **E-mail** all inquiries to both Procurement Officers listed above, no later than 4:00 PM EST on February 10, 2021. **All questions must be submitted in writing.** Responses to questions will be posted on the Mason Purchasing Website by 4:00 PM EST on February 17, 2021. Note: Questions must be submitted in WORD format. Also see section III. COMMUNICATION, herein.

PROPOSAL DUE DATE AND TIME: February 24,2021 @ 2:00 PM EST. **SEE SECTION XIII.A.1 FOR DETAILS ON ELECTRONIC PROPOSAL SUBMISSION.**

In Compliance With This Request For Proposal And To All The Conditions Imposed Therein And Hereby Incorporated By Reference, The Undersigned Offers And Agrees To Furnish The Goods/Services In Accordance With The Attached Signed Proposal Or As Mutually Agreed Upon By Subsequent Negotiations.

Name and Address of Firm:

Legal Name: Cotton & Company LLP

DBA: N/A

Address: 333 John Carlyle Street, Suite 500

Alexandria, Virginia 22314

FEI/FIN No. 54-1172176

Fax No. 703.836.0941

Email: MMesko@cottoncpa.com

Date: February 24, 2021

By: [redacted]
Signature

Name: Megan Mesko, CPA, CFE

Title: Partner

Telephone No. 703.836.6701

SWaM Certified: Yes: X No: _____ (See Section VII. SWaM CERTIFICATION for complete details).

SWaM Certification Number: 704647

This public body does not discriminate against faith-based organizations in accordance with the *Governing Rules, § 36* or against a Bidder/Offeror because of race, religion, color, sex, national origin, age, disability, or any other prohibited by state law relating to discrimination in employment.

1.B. Small Business Subcontracting Plan [RFP Section XIII, Paragraph B.1.b. Return Attachment A – Small Business Subcontracting Plan]

We have provided our small business subcontracting plan on the following page.

ATTACHMENT A
SMALL BUSINESS SUBCONTRACTING PLAN
TO BE COMPLETED BY OFFEROR

It is the goal of the Commonwealth that over 42% of its purchases be made from small businesses. All potential offerors are required to include this document with their proposal in order to be considered responsive.

Small Business: "Small business (including micro)" means a business which holds a certification as such by the Virginia Department of Small Business and Supplier Diversity (DSBSD) on the due date and time for proposals. This shall also include DSBSD certified women- owned and minority-owned businesses and businesses with DSBSD service disabled veteran owned status when they also hold a DSBSD certification as a small business on the proposal due date. Currently, DSBSD offers small business certification and micro business designation to firms that qualify.

Certification applications are available through DSBSD online at www.SBSD.virginia.gov (Customer Service).

Offeror Name: Cotton & Company LLP

Preparer Name: Megan Mesko, CPA, CFE, Partner **Date:** February 24, 2021

Who will be doing the work: □ I plan to use subcontractors X I plan to complete all work

Instructions

A. If you are certified by the DSBSD as a micro/small business, complete only Section A of this form.

B. If you are not a DSBSD-certified small business, complete Section B of this form. For the proposal to be considered and the offeror to be declared responsive, the offeror shall identify the portions of the contract that will be subcontracted to DSBSD certified small business for the initial contract period in relation to the offeror's total price for the initial contract period in Section B.

Section A

If your firm is certified by the DSBSD provide your certification number and the date of certification.
Certification Number: 704647 Certification Date: February 14, 2019

Section B

If the "I plan to use subcontractors" box is checked, populate the requested information below, per subcontractor to show your firm's plans for utilization of DSBSD-certified small businesses in the performance of this contract for the initial contract period in relation to the offeror's total price for the initial contract period. Certified small businesses include but are not limited to DSBSD-certified women-owned and minority-owned businesses and businesses with DSBSD service disabled veteran-owned status that have also received the DSBSD small business certification. Include plans to utilize small businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc. It is important to note that these proposed participation will be incorporated into the subsequent contract and will be a requirement of the contract. Failure to obtain the proposed participation dollar value or percentages may result in breach of the contract.

B. Plans for Utilization of DSBSD-Certified Small Businesses for this Procurement

Subcontract #1

Company Name: _____ SBSD Cert #: _____
Contact Name: _____ SBSD Certification: _____
Contact Phone: _____ Contact Email: _____
Value % or $ (Initial Term): _____ Contact Address: _____
Description of Work: _____

Subcontract #2

Company Name: _____ SBSD Cert #: _____
Contact Name: _____ SBSD Certification: _____
Contact Phone: _____ Contact Email: _____
Value % or $ (Initial Term): _____ Contact Address: _____
Description of Work: _____

2. GENERAL FIRM BACKGROUND AND INFORMATION [RFP SECTION XIII, PARAGRAPH B.2. GENERAL FIRM BACKGROUND AND INFORMATION]

2.A. BACKGROUND AND HISTORY OF FIRM [RFP SECTION XIII, PARAGRAPH B.2.A. PROVIDE A BACKGROUND AND BRIEF HISTORY OF YOUR FIRM]

Cotton & Company LLP is a certified public accounting partnership headquartered in Alexandria, VA. We are licensed and in good standing with the Commonwealth of Virginia, the State of Maryland, and the District of Columbia, and we are qualified to practice in all other jurisdictions. Since our founding in 1981, Cotton & Company has focused our practice on providing audit, accounting, litigation support, information assurance, and management consulting services, primarily serving the federal government.

Cotton & Company is committed to serving the public interest, exceeding client expectations, and providing career-enhancing opportunities for our personnel. To achieve these goals, we focus on three key philosophies:

- **Quality.** Our commitment to quality is second to none. Since our founding in 1981, Cotton & Company has focused both on quality within the firm and on efforts to improve the management of quality within our profession. We began participating in a peer review program in 1983—7 years before quality reviews became mandatory for CPA firms. Cotton & Company maintains a rigorous quality management system that exceeds the quality control and assurance requirements established in *Government Auditing Standards*. Firm partners have served on various professional ethics committees to improve the quality of our profession, and they remain at the forefront of these quality improvement efforts. In 2007, we became one of the first accounting firms in the U.S. to voluntarily undergo annual peer reviews, subjecting our professional practice to more frequent reviews and thereby ensuring we provide the highest professional and ethical standards. Moreover, although not required to do so, we voluntarily include our performance audits in the scope of our peer reviews.

  Cotton & Company completed external peer reviews every 3 years from 1984 through 2008, and we consistently received an unqualified opinion with no letter of comment. Under the new standards (effective January 1, 2009), we have received a peer review rating of "pass"—the highest possible rating— each year since 2008.

- **Experience.** We offer Mason's Office of Audit, Risk, and Compliance a team of highly qualified professionals that have dedicated their careers to providing services similar to those requested; in particular, our personnel have extensive experience assessing institutes of higher education's (IHEs') compliance with both internal and external policies and regulations. We have considerable and varied experience with industry standards/ benchmarks and best practices, including, but not limited to generally accepted accounting principles (GAAP); Generally Accepted Government Auditing Standards (GAGAS); Office of Management and Budget (OMB) Circulars, Bulletins, and Memoranda, including the Code of

Federal Regulations (CFR); legislative requirements; and Government Accountability Office (GAO) guidance on internal controls.

- **Commitment.** Cotton & Company values each of our clients and every contract, as evidenced by our many repeat clients and by the wide range of services that we often provide to a single client. We demonstrate our commitment not only through the high quality of our technical work, but also through our customer-oriented approach. In every engagement, Cotton & Company's commitment to our clients ensures we support them in meeting their objectives while also continuously striving to gain improvements and increased efficiencies. This commitment includes partner assignment and involvement on every single engagement, both large and small.

2.B. Firm Specialties [RFP Section XIII, Paragraph B.2.b. Describe your firm's specialty areas, and their size]

Once a small business providing grant and contract audits to federal clients with a handful of auditors, Cotton & Company has grown to a firm of 16 partners and more than 180 employees providing a full range of audit, accounting, information system, and management consulting services to both federal and non-federal entities. We aim to continuously expand both our client base and our range of services, and we have conducted thousands of financial, performance, and compliance audits of government financial statements, contracts, grants, programs, and agencies. Cotton & Company also performs information technology (IT) systems and security audits, evaluations, and reviews and provides financial management consulting services to federal government Chief Financial Officers (CFOs) to assist with audit readiness and remediation, OMB Circular A-123 compliance, CFO Act audit deliverables, and other Treasury and OMB requirements. Finally, the firm provides litigation support and forensic accounting services to assist our clients in evaluating contract matters and disputes.

Cotton & Company's credentials that are most relevant to the proposed engagement include:

- Extensive experience conducting performance audits and compliance reviews of IHEs, not-for-profit organizations, and hospitals for various federal and non-profit organizations.
- Prior experience providing co-sourcing services to Mason's Controller's Office and Office of University Audit.
- Significant experience with construction projects, including performance audits of local government construction management practices, construction claim audits and reviews, construction auditing services, and a risk assessment of a state agency's construction management program.
- Significant knowledge of state laws and federal regulations, including experience establishing procedures and processes to comply with these regulations.
- More than 180 experienced personnel, giving us the staffing resources to perform any type of engagement. This includes more than 50 information assurance (IA) professionals with experience performing information security, privacy, and operational audits.

2.C. FIRM LOCATION AND STRUCTURE [RFP SECTION XIII, PARAGRAPH B.2.C. DESCRIBE YOUR FIRM'S LOCATION AND ORGANIZATION STRUCTURE. PROVIDE ADDITIONAL DETAIL RELATED TO OFFICES LIKELY TO SERVE MASON.]

Cotton & Company's only office is located in Old Town Alexandria, less than 30 minutes from Mason's Fairfax campus. This proximity makes our team easily accessible and ensures our personnel will be available to provide on-site services as necessary, with little advance notice.

Cotton & Company has 16 partners with diverse backgrounds, interests, and talents, which enables our firm to provide quality services within three main practice groups: Contracts, Grants, and Litigation (CGL); Assurance, and Advisory. These practice groups would all be available to assist with the requested services.

2.c.1. Contracts, Grants, and Litigation (CGL) Practice

Cotton & Company's skilled CGL auditors are well suited to perform the requested internal audit services. Since the firm's founding, the CGL Practice group has performed thousands of incurred-cost audits, performance audits, pre-award audits, indirect cost rate audits, financial-related audits, and agreed-upon procedures (AUPs) reviews for more than two dozen federal Inspectors General (IGs), as well as for IHEs, state agencies, not-for-profit entities, and commercial organizations. Specifically, this group has extensive experience:

In addition to reviewing costs claimed by hundreds of IHEs, not-for-profit entities, and hospitals, this team has provided co-sourcing services to Mason, audit/consulting services to New York University, and construction claim analysis services to Rutgers University.

- Performing financial, performance, and compliance audits of government contracts and grants awarded to IHEs to determine whether costs incurred are reasonable, allocable, eligible, and allowable in accordance with laws, regulations, and contract terms and conditions.
- Conducting audits of contractor/grantee indirect cost rates.
- Providing construction project-related services, including construction claim audits and reviews, litigation support services related to construction claims, and performance audits of state and federal construction management practices.
- Performing pre-award audits to determine whether prospective contractors have adequate accounting systems and the financial capability to perform contracts.
- Conducting data mining and data analytics to identify transactions that represent anomalies, outliers, and aberrant transactions.
- Assisting in fraud investigations, including fraud hotline investigations.
- Performing forensic reviews.
- Providing audit support.

COTTON & COMPANY'S CGL SUBJECT MATTER EXPERTS (SMES)

[redacted]
Grant and Contract Compliance, Data Analytics

[redacted]
Construction Audit Services, Fraud Investigations

[redacted]
Construction Litigation, Forensic Reviews

2.c.2. Assurance Practice

Cotton & Company's Assurance professionals are well suited to perform a wide range of audits. In particular, we have a team of IT auditors prepared to support Mason. Our team has extensive experience providing a range of IT and cybersecurity audits, including:

Cotton & Company has applied to become a Certified Third-Party Assessor Organization (C3PAO) through the Certified Maturity Model Certification (CMMC) Accreditation Body. Once approved, this designation will allow us to perform CMMC assessments.

- Evaluating an entity's overall cybersecurity posture.
- Evaluating an entity's identity and access management, including its privileged account management.
- Conducting privacy audits focused on evaluating the entity's controls over identifying and protecting personally identifiable information (PII).
- Conducting targeted advanced threat audits, including evaluating firewall configuration and rules, security event information management tools, and associated processes performed by the entity's security operations center.
- Auditing an entity's operating system configuration, including Windows Active Directory and Unix/Linux configurations and controls.
- Evaluating an entity's business continuity and associated disaster recovery plans.
- Evaluating an entity's transition to cloud and outsourced environments, including its cloud strategy and governance.
- Performing audits to address an entity's compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 1*, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.*
- Conducting performance audits aimed at improving program performance and operations, reducing costs, facilitating decision-making by parties responsible for overseeing or initiating corrective action, and contributing to public accountability.

ASSURANCE SUBJECT MATTER EXPERTS (SMES)

[redacted]
Data Protection and Privacy

[redacted]
Identity and Access Management

[redacted]
Cloud Governance and Implementation

2.c.3. Advisory Practice

Cotton & Company's financial management and IA professionals in its Advisory practice have years of experience working with comptrollers and Chief Information Officers (CIOs) to help establish and maintain programs that meet and exceed the internal control requirements specified in OMB Circular A-123. Further, because Cotton & Company has received Registered Provider Organization (RPO) accreditation from the CMMC Advisory Board, this practice group is positioned to provide Mason with CMMC advisory support. Specifically, this group has extensive experience:

- Providing audit support and remediation services.
- Offering accounting and budget execution support.
- Documenting and designing policies and procedures.
- Developing, implementing, and monitoring corrective action plans (CAPs).
- Performing pre-assessments to help identify corrective actions or implementation gaps for the required cybersecurity controls.

ADVISORY SUBJECT MATTER EXPERTS (SMES)

[redacted]
CIO Internal Audit Support

[redacted]
CMMC Advisory Support

[redacted]
Enterprise Risk Management

2.D. RELEVANT EXPERIENCE WITH IHES AND RESEARCH INSTITUTIONS [RFP SECTION XIII, PARAGRAPH B.2.D. DESCRIBE THE NATURE AND EXTENT OF YOUR EXPERTISE WITH HIGHER EDUCATION, RESEARCH-ORIENTED, OR SIMILARLY-SITUATED CLIENTS, INCLUDING RELATED INFORMATION TECHNOLOGY ENVIRONMENTS (INCLUDING BANNER, WHICH IS USED BY MASON.)]

In addition to our experience using Banner while providing co-sourcing audit services to Mason, as described in the Relationships with Mason and Relevant IT Co-Sourcing and Audit Experience sections of this proposal, we have also provided information on two recent contracts that demonstrate the nature and extent of our expertise with higher education, research-oriented, and other similarly situated clients: the Patient-Centered Outcomes Research Institute (PCORI) and the National Science Foundation (NSF) Office of Inspector General (OIG). In addition, we have also provided information on our ongoing contract with the Virginia Department of

Transportation (VDOT), which is an institution of the Commonwealth of Virginia and is therefore subject to many of the same regulations that are applicable to Mason. These clients most aptly demonstrate the solid base of knowledge and experience that Cotton & Company will bring to Mason, as well as our longstanding commitment to our clients.

2.d.1. Patient-Centered Outcomes Research Institute (PCORI)

PCORI is a non-profit organization funded through the Patient-Centered Outcomes Research Trust Fund, which was established by the U.S. Congress through the Patient Protection and Affordable Care Act of 2010 (PPACA). PCORI has awarded more than $2.8 billon to fund more than 1,700 research projects.

PCORI engaged Cotton & Company in 2016 to develop a risk matrix of PCORI contractors and to assist PCORI in performing compliance reviews designed to demonstrate to GAO that PCORI was appropriately monitoring its significant research portfolio. Under our current Master Service Agreement (MSA) with PCORI, Cotton & Company provides co-sourcing, consulting, and external compliance review services. These services have provided Cotton & Company's CGL team with the opportunity to work with dozens of IHEs, not-for-profit entities, and hospitals that use a variety of IT systems (e.g., Banner, Oracle, Workday).

Based on our understanding of PCORI's internal policies and contract/award requirements, we assisted PCORI in establishing its first compliance review program in 2016. PCORI then contracted Cotton & Company to (1) perform reviews under its pilot program, (2) execute dozens of reviews each year as part of PCORI's external compliance review program, and (3) assist PCORI in continuously updating its compliance review approach to increase the efficiency of its monitoring and reduce the burden on awardees. Since this program began in 2016, Cotton & Company has completed 89 compliance reviews of contracts awarded to 53 IHEs, hospitals, and non-profit research organizations managing PCORI awards, many of which use Banner financial systems.

Although our MSA is with PCORI's Finance department, we meet with personnel within PCORI's Science and Contracts Management departments during each phase of our compliance reviews to ensure that PCORI personnel have a consistent understanding of the purpose of these reviews and appropriately convey this understanding to the organizations under review.

2.d.2. National Science Foundation (NSF) Office of Inspector General (OIG)

Cotton & Company has performed financial and compliance audits and other audit services for the NSF OIG on a task order basis since 1987. Specific tasks requested have included financial and compliance audits of grants and contracts awarded to nonprofit organizations, state and local governments, colleges and universities, for-profit organizations, and national associations. Most grantees audited had multiple subgrantees,

Cotton & Company uses IDEA as our primary data analytics software; however, our employees have experience executing data analytics using IDEA, ACL, Alteryx, Dundas, Tableau, and PowerBI.

and audit scopes included full- or limited-scope reviews of subgrantee records. Many of these subgrantees operate through fiscal agents (e.g., colleges, universities, local governments).

Most relevantly, under Cotton & Company's current 5-year Blanket Purchase Agreement (BPA), our CGL team has performed or is currently performing 20 audits of costs claimed by 20 IHEs. Ten of these audits have involved a preliminary survey phase, in which our team evaluates the grantee's award management environment and creates an organizational risk assessment, which we use to determine whether we should perform any further audit testing. To create the organizational risk assessment, the Cotton & Company team evaluates the strengths and weaknesses of each of the IHE's internal controls within each NSF budget category. Our team also performs various analytics on Banner and other financial system data to identify anomalies in the organization's accounting system data and tests a sample of judgmentally selected transactions.

The other 10 audits have involved gaining an understanding of the IHEs' implementation of various flexibilities that OMB granted in response to the Coronavirus Disease 2019 (COVID-19) pandemic. These limited-scope performance audits involve conducting interviews to evaluate whether—and how—IHEs implemented the COVID-19 flexibilities, using a data analytics approach to conduct judgmental testing of expenses incurred in accordance with the COVID-19 flexibilities, and evaluating whether the IHE's implementation of the flexibilities conforms with applicable federal guidance and NSF terms and conditions.

By performing audits that require gaining an understanding of how IHEs implemented the flexibilities that OMB granted in response to the COVID-19 pandemic, Cotton & Company has gained unique insight into best practices for ensuring compliance in this emerging risk area impacting higher education.

2.d.3. Virginia Department of Transportation (VDOT)

Cotton & Company has provided consultant audit services to VDOT since 2011 under three BPAs and numerous task orders. Most relevantly, Cotton & Company has successfully provided construction-related consulting services to VDOT's Assurance and Compliance Office (ACO), including:

These consulting services are not specifically related to higher education or research; however, because VDOT is also an institution of the Commonwealth of Virginia, it is subject to many of the same regulations that apply to Mason.

- **Construction Project Claims Review:** Cotton & Company analyzed a contractor's delay, remobilization, and escalation claims resulting from a VDOT construction project. We issued two reports to VDOT that questioned approximately $3.3 million of the contractor's claimed amounts based on our determination that the questioned costs were duplicative of other claims, were included in the original scope of work, and/or were not reasonable or adequately supported.
- **Construction Risk Management:** Cotton & Company currently performs a risk assessment of VDOT's construction management program, focusing on capital projects funded with

state and federal funding. Cotton & Company teamed with an engineering firm on this engagement to obtain relevant expertise in identifying risks and recommendations related to the technical aspects of the projects. At the end of this engagement, Cotton & Company will provide VDOT with findings and recommendations to improve VDOT's management of its project costs, timeliness, and risk.

- **Work Order Reviews:** Cotton & Company currently reviews work orders that VDOT awarded to numerous contractors on various VDOT construction projects. The work includes reviewing the work order requests that the contractors submitted and the amounts that VDOT awarded to ensure the awarded amounts were reasonable, allowable, and allocable to the construction project. Cotton & Company also ensures these awards were based on costs that the contractors actually incurred, were for work that was not duplicative of the original contract scope, and complied with both the Federal Acquisition Regulation (FAR) and the terms of the contract.

2.E. RELEVANT AUDIT CO-SOURCING EXPERIENCE [RFP SECTION XIII, PARAGRAPH B.2.E. DESCRIBE THE NATURE AND EXTENT OF YOUR EXPERTISE WITH PROVIDING SUPPLEMENTAL AUDIT RESOURCING (CO-SOURCING) SERVICES TO CLIENTS SIMILARLY-SITUATED TO MASON.]

In addition to our previous experience providing co-sourcing audit, accounting, and IT services to Mason, as described in Relationships with Mason, Cotton & Company has extensive expertise with providing supplemental resourcing (co-sourcing) services, including construction audit services, for other, similarly situated clients. Below, we provide information on our relevant co-sourcing experience in different areas.

2.e.1. CGL Co-Sourcing Experience

Below, we provide information on three recent contracts that demonstrate the nature and extent of our CGL team's expertise with regard to relevant services. These contracts include services provided to the U.S. Capitol Police (USCP) OIG, Architect of the Capitol (AOC) OIG, and PCORI.

2.e.1.a. U.S. Capitol Police (USCP) OIG

Cotton & Company has provided audit and investigative services for the USCP OIG since 2008 under indefinite delivery/indefinite quantity (IDIQ) contracts with time-and-materials work orders. Starting in fiscal year (FY) 2017, Cotton & Company also began providing audit support staff and quality control reviews to assist the OIG in performing the annual audit of USCP's financial statements. The scope of our work includes:

- Performing financial audits, performance audits, expanded-scope audits, indirect-cost audits, and other types of audits of USCP programs and operations.

- Performing pre-award surveys, pricing reviews, quality control reviews, evaluations, analyses, and follow-ups of USCP programs and operations.
- Conducting surveys, providing technical assistance, and preparing audit plans and reports.
- Conducting investigative work under the purview and oversight of OIG investigations.
- Providing technical aid and training.
- Performing inspections, evaluations, reviews, and analyses.
- Providing professional individuals to assist the OIG in conducting audits, inspections, evaluations, reviews, and analyses.
- Providing professional individuals for select tasks (e.g., referencing audit projects) to aid the OIG in performing work under the IDIQ contract.

The performance audits, AUP engagements, and special audit services that Cotton & Company has performed for the USCP OIG cover a wide range of areas, including time and attendance, program integrity, internal controls over compliance, adherence to policies and procedures, and information security. In performing these engagements, we leverage our corporate experience and the experience of our audit team members to identify and incorporate industry best practices into our audit methodologies, findings, and recommendations.

2.e.1.b. Architect of the Capital (AOC) OIG

Cotton & Company currently provides construction project services for the AOC OIG, including serving as a SME in assessing AOC's construction management processes and conducting performance audits related to AOC's million-dollar multi-year construction project to rehabilitate the Cannon House Office Building on Capitol Hill.

Because construction project schedules leave little flexibility for the project team, Cotton & Company plans and adjusts our audit schedule to account for busy periods on the project. We can ramp up our audit work to quickly review documentation once it is available, ensuring that audits remain on schedule and reducing the burden on the construction project teams under audit.

Specifically, Cotton & Company conducted a performance audit to assess whether modifications to AOC's contract for Cannon House Office Building improvements were reasonable, necessary, within the scope of the contract, and effectively awarded and administered. Cotton & Company's specific responsibilities included obtaining an understanding of AOC's policies and procedures for the contract modification process; assessing AOC's internal controls for contract modifications; reviewing a sample of the contract modifications, amendments, and change orders that affected the original contract value to determine the reason for and the necessity of the changes; assessing the reasonableness of price changes; and assessing the sufficiency of AOC's oversight of the contract.

Cotton & Company also conducted a performance audit to assess AOC's review and approval of the Cannon Renewal Project invoices to ensure the costs and payments complied with contract

requirements, AOC policies and procedures, and industry standards. The audit also determined whether the costs invoiced were allowable, supported, and reasonable within the scope of contract requirements. Our team's specific responsibilities included obtaining an understanding of AOC's contract requirements and policies/procedures for contract invoices, as well as assessing AOC's internal controls for the review, approval, and payment of contract invoices.

In addition to performing audits for the AOC OIG, Cotton & Company currently serves as a SME assessing AOC's monthly and semiannual progress reports for the Cannon House Office Building Renewal Project. Specially, Cotton & Company reviews the project reports to determine whether the project is progressing in a timely and cost-effective manner and summarizes these findings. Our limited review focuses on the scope, safety, budget, schedule, and cost schedule risk assessments that AOC reports on.

2.e.1.c. Patient-Centered Outcomes Research Institute

In addition to the extensive experience with higher education and research-oriented organizations we have gained as a result of performing compliance reviews for PCORI, Cotton & Company has also provided a variety of co-sourcing services to PCORI's financial compliance team under our current MSA. Specifically, since 2016 Cotton & Company has provided PCORI with both full- and part-time staff augmentation services to assist PCORI in achieving both its short-term and long-term financial compliance goals. In particular, we have provided PCORI with additional staff upon request to assist with contract close-out activities, internal compliance review procedures, and data validation activities (including verifying contract budgets, cumulative amounts spent, and awardee/contract terms and conditions) during PCORI's transition to a new database software.

Further, Cotton & Company provides consulting services to PCORI on an as-needed basis to assist its financial compliance team in updating its compliance review program. These activities have included developing a new external compliance review program in 2020, assisting in the design of a pre-award questionnaire PCORI uses to help assess systemic risk at institutions seeking new funding, providing recommendations for updates to PCORI's allowable cost guidelines, and developing a handout designed to help awardees prepare for a successful compliance review.

Cotton & Company holds regular meetings to discuss the results of our compliance reviews with PCORI's Finance, Contracts Management and Administration, and Science leadership teams to ensure PCORI can use our independent observations to add value and improve its internal operations across all of its departments.

Cotton & Company also developed and continuously updates the risk matrices that PCORI uses to identify contracts and awards that represent the most significant threats to the organization. We use these risk matrices to perform an annual risk assessment, then meet with the PCORI financial compliance team to review the results and determine which contract(s) or institutions PCORI should review during the next fiscal year.

2.e.2. Relevant IT Co-Sourcing and Audit Experience

Our IA professionals also have substantial experience providing IT-related co-sourcing services, including providing services to Mason's Office of Audit, Risk and Compliance team. Below, we provide information on three recent contracts that demonstrate the nature and extent of our IA team's expertise with regard to relevant services. These contracts include services provided to Mason's Office of Audit, Risk and Compliance, the Federal Deposit Insurance Corporation (FDIC) OIG, and the Library of Congress (LOC) OIG.

2.e.2.a. George Mason University Office of Audit, Risk, and Compliance

Mason's Office of Audit, Risk and Compliance engaged Cotton & Company to provide an experienced IT auditor to conduct testing of controls required by NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. This testing validated whether the controls that Mason implemented in its newly deployed Controlled Unclassified Information (CUI) environment met NIST 800-171 standards. The areas of focus included:

- Access Controls
- Audit and Accountability
- Configuration Management
- Risk Assessment
- Systems and Communications Protection
- System and Information Integrity

As a recipient of Department of Defense (DoD) funds, Mason will be required to undergo the CMMC assessment process. As a DoD-approved RPO, Cotton & Company is able to support Mason in these efforts.

Mason deployed this new CUI environment to enable its personnel to apply for federal government research awards. Cotton & Company:

- Produced workpapers to support the work performed. These workpapers were substantially similar to those the Office of University Audit normally prepares.
- Documented our understanding of the controls and their effectiveness that we obtained during testing.
- Documented any evaluations or conclusions we formed through our testing.

As a result of our testing, we identified gaps in Mason's compliance with NIST SP 800-171 in the areas noted above.

2.e.2.b. Federal Deposit Insurance Corporation (FDIC) OIG

Cotton & Company has performed IT, cybersecurity, and operational audits and other audit services for the FDIC OIG on a task order basis since 2015. Specific tasks requested have included the following audits:

- **Federal Information Security Modernization Act (FISMA):** Cotton & Company has performed cybersecurity audit services in support of the FDIC OIG's responsibilities under FISMA for the last 6 years. We have performed the FISMA audit and issued a performance audit report every year since 2015. The FISMA audit addresses primary cybersecurity topics, including identity and access management, protection of PII, contingency planning, information system and enterprise risk management, hardware and software inventory, configuration management, and information systems continuous monitoring.

- **Enterprise Risk Management (ERM):** During one of our FISMA audits for the FDIC OIG, we noted issues related to ERM. Based on that work, the FDIC OIG asked us to support its performance audit evaluating the ERM program and processes at the FDIC.

- **Regional Automated Document Distribution and Imaging System (RADD):** In 2018, the FDIC OIG engaged Cotton & Company to perform an audit of security controls over the RADD system, a major application that the FDIC developed in-house to support its examinations of financial institutions. The work included assessing the effectiveness of selected security controls designed to protect the confidentiality, integrity, and availability of information.

- **Advanced Persistent Threats:** In 2018, we performed an audit of the FDIC's ability to detect and respond to advanced persistent threats. Our team reviewed the configurations and related processes for firewalls and the FDIC's Security Incident and Event Management (SIEM) tool. Based on the results of our testing, we provided the FDIC OIG with a report on current and relevant threats.

- **Mobile Device Management and Governance:** In 2019, we performed an audit to assist the FDIC OIG in assessing the FDIC's management and security of two agency-issued mobile devices—Apple iPhones and iPads—as well as the associated cloud-based mobile device management platform that the FDIC had implemented.

Cotton & Company is committed to customer satisfaction and quality through partner involvement, as evidenced by our most recent Contractor Performance Evaluation and Reporting Form (CPER) evaluation, issued for the 2019 FISMA audit. The FDIC OIG stated: [redacted] *demonstrated an excellent ability to communicate complex issues to OIG and FDIC management.* [redacted] *was highly committed to the success of this project and meeting the OIG's needs.* [redacted] *was critical to the Contractor's success on this project.*

- **Windows Active Directory:** In 2020, Cotton & Company began conducting a performance audit to assist the FDIC OIG in determining whether the FDIC had designed and implemented effective controls to protect network systems and data for its Windows Active

Directory. This audit will include evaluating configuration of the FDIC's Windows Active Directory, as well as performing an internal penetration test of the FDIC's Windows environment and password-cracking of its Windows Active Directory passwords.

2.e.2.c. Library of Congress (LOC) OIG

Since September 2017, Cotton & Company has conducted a number of performance audits, reviews, and other audit services for the LOC OIG. We conduct these engagements in accordance with GAGAS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation*, as applicable. Specific examples of engagements that Cotton & Company has performed for LOC include:

Cotton & Company's CGL Practice has also provided a variety of non-IT performance audit and review services for the LOC OIG since 2017, including grant audits, an audit of selected contracts, hotline complaint reviews, and a fraud review.

- **U.S. Copyright Office (USCO) IT Modernization Plan Audit.** Cotton & Company conducted a performance audit of LOC's IT modernization project related to the Copyright Recordation System. The objectives of this engagement included concluding on whether the LOC Office of the Chief Information Officer (OCIO) and USCO complied with LOC's policies and procedures related to the systems development life cycle (SLDC) and project management life cycle (PMLC), as well as whether the project was on schedule and within budget. We also reviewed and analyzed the Contracting Officer's Representative's (COR's) function in LOC's IT modernization efforts.

- **Library Services SDLC/PMLC Review.** The LOC OIG engaged Cotton & Company to conduct a performance audit of LOC's IT modernization project related to the Merged Audio-Visual Information System (MAVIS). The objective of this engagement is to evaluate Library Services and OCIO's project management and software development practices using GAO's *Schedule Assessment Guide, Cost Estimating and Assessment Guide*, and *Software Development: Effective Practices and Federal Challenges in Applying Agile Methodologies*.

- **Cloud Governance Audit.** The LOC OIG engaged Cotton & Company to conduct a performance audit to determine whether LOC had implemented adequate governance controls to enable secure and operationally suitable cloud services that are cost-beneficial to the agency. The objectives of this engagement include determining whether LOC prioritized and completed an enterprise-wide cloud strategy that aligned with federal guidance; whether LOC's cloud inventory is accurate, formalized, and managed using automated methods; and whether LOC effectively implemented federal standards and requirements and best practices for its existing cloud implementations.

2.F. Impending Organizational Changes [RFP Section XIII, Paragraph B.2.F. Describe any impending changes in your organization that could impact delivery of services.]

Cotton & Company has responded to the impact of the Coronavirus Disease 2019 (COVID-19) by following both local and federal guidance for continued operations. We remain vigilant to ensure the health and welfare of our employees, contractors, and clients. To that end, although we do not have any impending organizational changes, the majority of our employees have been teleworking since May 2020, rather than commuting to the Cotton & Company office or to one of our 63 client sites.

Further, Cotton & Company has the necessary expertise and experience to assist federal and state agencies and their IGs with ensuring accountability and spending transparency for funds related to COVID-19 aid, relief, and response. The historic size and scope of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) funding—coupled with the expediency and flexibility needed to distribute the funds to meet critical needs—calls for increased risk management, monitoring, reporting, and oversight of federal spending. Cotton & Company's decades of relevant experience ensure that we can support our clients as needed.

3. RELATIONSHIPS WITH MASON [RFP SECTION XIII, PARAGRAPH B.3. RELATIONSHIPS WITH MASON]

Since January 1, 2018, Cotton & Company has provided co-sourcing services to Mason under three purchase orders issued by two offices: the Office of Audit, Risk and Compliance and the Controller's Office. For these engagements, Cotton & Company was able to provide well-qualified assurance and CGL staff to provide temporary support services as needed, on a variable hours-level basis.

We provide additional information about each of these engagements below.

3.A. List of Work Cotton & Company Has Conducted Related to Mason [RFP Section XIII, Paragraph B.3.A. Provide a list of work your firm has conducted related to Mason since January 1, 2018. Describe the nature of the work, cost, and Mason contact.]

IT Audit Support	
Nature of the Work	Cotton & Company provided an experienced IT auditor to conduct testing of controls required by NIST SP 800-171, *Protecting Controlled Unclassified Information in nonfederal Systems and Organizations*. This testing validated whether the controls that Mason implemented in its newly deployed CUI environment met NIST 800-171 standards.
Period of Performance	[redacted]
Cost	[redacted]

Mason Contact	[redacted]	Janatry E. Sanders, CISSP, CISA, CAP, Auditor jsander6@gmu.edu | (703) 993-3130

NCAA and Other Audit Assistance	
Nature of the Work	Cotton & Company provided an experienced senior auditor to provide temporary audit and financial analysis support services to Mason under the direction of the Associate Controller.
Period of Performance	[redacted]
Cost	[redacted]
Mason Contact	Claire Wurmfeld, Associate Controller cwurmfel@gmu.edu | 703-993-5328

General Accountant Services	
Nature of the Work	Cotton & Company provided two experienced IA staff to: • Assist the Associate Controller in analyzing Mason's current financial reporting activities. • Assist with process development to produce quarterly financial statements and board/management reports. • Help evaluate current reconciliation methods (i.e., actuals and budget to actuals) and systems (e.g., Banner Finance/MicroStrategy) to recommend improvements to processes and procedures, as requested.
Period of Performance	[redacted]
Cost	[redacted]
Mason Contact	Claire Wurmfeld, Associate Controller cwurmfel@gmu.edu | 703-993-5328

4. MANAGING THE RELATIONSHIP WITH MASON'S OFFICE OF AUDIT, RISK, AND COMPLIANCE [RFP SECTION XIII, PARAGRAPH B.4. MANAGING THE RELATIONSHIP WITH MASON'S OFFICE OF AUDIT, RISK, AND COMPLIANCE]

Cotton & Company has many repeat clients, which we consider evidence of our outstanding, timely performance and our sustained ability to develop effective relationships and exceed client expectations. We will develop an effective working relationship that enables us to deliver quality services to Mason's Office of Audit, Risk, and Compliance by ensuring that we efficiently manage and staff this contract and each individual task order.

4.A. PROCESS FOR WORKING WITH MASON'S OFFICE OF AUDIT, RISK, AND COMPLIANCE [RFP SECTION XIII, PARAGRAPH B.4.A DESCRIBE YOUR PROCESS FOR WORKING WITH MASON'S OFFICE OF AUDIT, RISK, AND COMPLIANCE TO DELIVER SERVICES. AMONG OTHER THINGS, DESCRIBE:]

Below, we discuss various aspects of Cotton & Company's process for working with our clients.

4.a.1. Knowledge, Skills, and Capacity [RFP Section XIII, Paragraph B.4.a.1 Knowledge, skills, and expected availability/capacity to deliver services]

Cotton & Company recognizes the effort needed to accomplish the scope of work identified in this solicitation, and we are ready and able to perform the requested services. In managing our resources to ensure comprehensive coverage across the requested services, the engagement partner will match individual qualifications and skill sets of assigned personnel to the complex engagement requirements. Our diverse workforce, strong management, and reputation for quality work under all circumstances enable us to smoothly transition our employees from one client to another. Combined with our continuous recruiting efforts, we can ensure a consistent flow of qualified candidates to fill additional and specified needs.

Cotton & Company's management strategy has been designed around a specialized environment that requires quick turnaround performance periods and flexible scheduling. Cotton & Company has a proven system for executing engagement awards, assigning appropriate personnel to engagements, and successfully managing engagement progress. We have used these procedures for nearly 40 years and have proven successful at managing numerous, varied, and ongoing task orders. We have found that the keys to providing high-quality services under these task orders include ensuring we have the right resources to complete the work and engaging in effective communication throughout each phase of each engagement.

4.a.2. Familiarity and Capability to Conform to International Standards for the Professional Practice of Internal Auditing [RFP Section XIII, Paragraph B.4.a.2. Familiarity and Capability to Conform to the International Standards for the Professional Practice of Internal Auditing.]

We understand that the International Standards for the Professional Practice of Internal Auditing consists of two categories: attribute and performance standards. These two categories address the attributes of organizations and individuals performing internal auditing, as well as provide quality criteria for use in measuring performance of internal audit services. These standards are consistent with the standards we use on every engagement, and all employees assigned to the requested services will follow these standards, as appropriate.

Individuals likely to provide these services include [redacted], who is a Certified Internal Auditor (CIA), and [redacted], CISSP, CISA. [redacted] is the current Chairman of the Board of the Northern Virginia Chapter of the Institute of Internal Auditors, where he also has served as a past President of the chapter.

4.a.3. Process for Scheduling Firm Resources [RFP Section XIII, Paragraph B.4.a.3. Process for scheduling firm resources to deliver services.]

Cotton & Company has processes and procedures in place to ensure that personnel complete tasks timely, are task-oriented, and have the appropriate time-management skills. The engagement partners are responsible for identifying:

- Activities to be performed for a particular task.
- The sequence and interdependencies among the activities.
- The type and quantity of resources needed.
- The estimated timeframes for completing the activities.

The engagement partners then develop a schedule and monitor the actual progress on the engagement against this schedule.

Cotton & Company's schedule management process will be closely integrated with Mason's own processes and tools for managing due dates. We will clearly communicate due dates to our personnel, as well as continuously monitor those due dates throughout the project.

Our schedule management process will be flexible and fluid to ensure continuous assessment and alignment of tasks to focus on the highest priority tasks—without sacrificing timely completion of other tasks. We will immediately evaluate and communicate impediments to timely completion of deliverables to make accommodations and minimize risk.

4.a.4. Supervision of Firm Resources [RFP Section XIII, Paragraph B.4.a.4. Supervision of firm resources should firm personnel be asked to supervise specific work.]

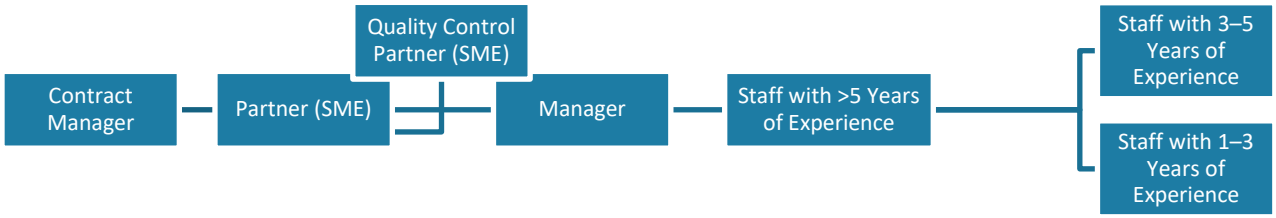
All Cotton & Company project teams have well-defined organizational structures with clear lines of authority and responsibility. We provide senior supervision at all levels of assignments (i.e., planning, fieldwork, workpaper review, and report preparation). Partners actively participate in all engagements, thus ensuring the highest possible level of attention within the firm to each assignment. As a result, team members understand engagement objectives and their responsibilities, assignments, and deadlines.

Below, we provide additional information regarding various aspects of Cotton & Company's process for supervising firm resources.

4.a.4.a. Organization of the Audit Team

Ms. Megan Mesko, a Cotton & Company partner, will serve as the contract manager for this engagement. She will have overall responsibility for supervising personnel and will serve as the principal liaison with Mason. Ms. Mesko will be responsible for assigning personnel—including

staff, managers, and SMEs—to task orders commensurate with their area and level of experience, as well as for ensuring all work is adequately supervised and all workpapers are reviewed, as detailed below. Although we will specifically tailor the staffing and supervision of firm resources based on the requirements of each engagement, we have provided a standard audit project organization chart below.



4.a.4.b. Oversight and Quality Controls for Deliverables

Cotton & Company's quality control and assurance philosophy addresses every segment of the firm's work, contributing to our product. This philosophy emphasizes the importance of exercising due professional care in conducting engagements and preparing related reports. Below, we discuss the segments of our quality assurance (QA) philosophy for deliverables.

- **Workpapers.** The quality of our workpapers directly reflects the quality of our team's supervision. Workpapers must contain enough support upon which to base a conclusion or opinion, as well as be legible, coherent, and clear. They serve a purpose beyond the mere preparation of the report; they also act as the organized repository for information that may be needed long after we have issued the report. The use of uniform formats encourages the systematic organization of workpapers during an engagement. It also allows ready access for reference, review, and orderly filing.

- **Workpaper Review and Report Processing.** Following completion of fieldwork, workpapers undergo three additional levels of quality control review, and reports undergo several editorial reviews. The in-charge senior or supervisor completes the workpapers, and a draft of the report is cross-indexed to the workpapers for the manager. The manager reviews the completed workpapers and reviews and edits the draft report. The manager documents all review comments and resolves the comments through consultation with the seniors and staff, as necessary. The partner-in-charge then reviews the completed workpapers, draft report, and all review worksheets, concentrating on the findings and supporting workpapers. The partner's review perspective encompasses the following:

    - Did the team meet the engagement objectives?
    - Did the team perform and document all required procedures?
    - Did the team cross-index all report elements to the sources and underlying workpapers?

- Did the team maintain evidence of compliance with all relevant standards and requirements?
- Is the report clearly written and theoretically and practically sound?
- Are conclusions and recommendations reasonable in relation to facts presented?

The engagement team then documents the partner's review and resolves all points before submitting the draft to our in-house Communications team for text processing and formatting. After the engagement team has resolved all review comments, the engagement partner signs and dates the workpaper cover(s). The Communications team then thoroughly edits the draft, and the partner accepts the changes. The team then cross-indexes the final draft to the underlying workpapers.

4.a.4.c. Oversight and Quality Control for Engagement Teams

As noted above, our staffing strategy consists of assigning appropriately experienced personnel who bring a wide range of experience to all engagements. It is essential to engagement success that we provide the requisite technical skills for every job. Consequently, we propose key personnel with relevant audit experience, many with agency-specific experience. Partners are heavily involved in engagement management to provide their unique, specialized perspectives to the process.

- **Hiring.** A professional service firm's most valuable assets are its personnel. The quality of a firm's hiring practices directly affects its performance. Cotton & Company expends considerable effort in screening and selecting our employees, and we specifically seek high levels of various positive attributes (e.g., intelligence, integrity, motivation, aptitude), in addition to work experience and academic background. Employment decisions are made at the highest level in the firm, reflecting their importance.
- **Advancement.** The key to continued individual and firm growth is the careful selection of deserving personnel for advancement to higher levels of responsibility. To this end, Cotton & Company conducts performance evaluations twice per year and at the end of major engagements. All individuals in the firm are evaluated, and salary adjustments are made annually solely on the basis of their performance evaluation, with advancement occurring when an individual displays the qualifications and motivation required for higher levels of responsibility. This commitment to providing our employees with rewarding opportunities is one of the many factors that resulted in *The Washington Post* naming Cotton & Company a Top Work Place in 2020.
- **Personnel Assignment.** The assignment of personnel is a critical task that directly impacts the firm's performance on a given engagement. Cotton & Company considers many factors in assigning personnel to individual tasks, including:
  - Stated requests for individuals by the client
  - Special expertise required
  - Engagement size and complexity

- Continuity of project teams
- Timing of the work to be performed
- Personnel availability
- Individual development

The engagement partner will approve all assignments with the goal of ensuring proposed staff members collectively possess adequate professional proficiency for the assignment.

- **Independence.** In all matters relating to audits, evaluations, and other services and the entities we serve, Cotton & Company is committed to remaining free from both personal and external impairment to independence, maintaining organizational independence, and maintaining an independent attitude and appearance.

  Per Cotton & Company policy, we do not consult where we audit, nor do we audit where we consult.

  - For each engagement, all team members are required to sign an "Engagement-Level Statement of Ethical Responsibilities" form stating that the team member has met their ethical responsibilities on the engagement, including maintaining independence. The team maintains this statement in the engagement workpapers, and the quality control partner reviews the statement before the team releases the final report.
- **Continuing Professional Education (CPE).** Cotton & Company requires audit and non-audit professional personnel to comply with GAGAS training and CPE requirements. All professional staff must complete at a minimum:
  - 80 hours of CPE every rolling two calendar years (at least 20 hours must be obtained in each of the two calendar years).
    - 24 of these 80 hours must be directly related to the government environment, government auditing, or other specific or unique environments in which we work.
  - Mandatory CPE requirements for the state(s) in which they are licensed.
- **On-the-Job Training:** On-the-job training is a significant aspect of professional development at Cotton & Company. Opportunities for this training occur in three ways:
  - In-charge personnel discuss with staff members their work in relation to the entire engagement, provide as much supervised responsibility as appropriate, explain every engagement step as it progresses, and answer questions.
  - Supervisors evaluate personnel in part by their effectiveness in properly training and developing subordinates.
  - Partners monitor assignments to ensure that personnel are fulfilling relevant experience requirements, gaining varied experience, assuming supervisory responsibility when appropriate, and working with many partners and managers.
- **Due Professional Care.** Cotton & Company exercises due professional care throughout all phases of an engagement. All personnel apply the care and skill expected of internal or

external auditors by considering the extent of work needed to achieve the engagement's objectives, the complexity of the matters under review, the adequacy and effectiveness of internal controls, and the probability of significant errors, fraud, or other non-compliance.

4.a.5. Capability and Process for Sharing Information [RFP Section XIII, Paragraph B.4.a.5. Capability, and related process, to share cross-industry and higher-education industry information related to (i) "best" practices, (ii) benchmarks, (iii) emerging higher education risk areas, (iv) internal audit practices, and (v) additional topics of interest.]

Through our extensive experience performing audits and compliance reviews at R1 and R2 research universities across the country, Cotton & Company has been able to gain unique insight into how universities with significant research activity can establish best practices and benchmarks, including how to develop effective monitoring of high risks and other areas of interest. To ensure our teams are continuously aware of emerging industry trends, updates to audit practices, and other areas of interest in the research community, Cotton & Company:

- ***Reviews Publications by Relevant Governing Organizations.*** Cotton & Company has monitoring controls in place within our business operations, quality control, and audit teams to ensure we are aware when relevant governing organizations (e.g., OMB, GAO, American Institute of Certified Public Accountants [AICPA]) publish guidance relevant to engagements we are performing, or may perform in the future. Most relevantly, in response to the COVID-19 pandemic, OMB issued memoranda that provided temporary administrative flexibilities for federal financial assistance awards, which NSF implemented. In addition to developing an audit plan that enabled us to gain an understanding of how IHEs implemented these flexibilities, we are also prepared to update any future audit programs that involve testing the allowability of costs incurred during the flexibility period that OMB granted.

- ***Attends and Presents at Higher Education Conferences.*** Cotton & Company staff often attend and present at university research administration-related conferences, including the National Council of University Research Administrators' (NCURA's) Financial Research Administration (FRA) Conference, the Association of College & University Auditors (ACUA's) Audit Interactive and AuditCon conferences, and the Society of Research Administrators International's (SRAI's) annual meetings. Examples of presentations that Cotton & Company personnel have performed include:

NCURA

- **Presentation Title:** *Questioned vs. Sustained, A Review of the Audit Resolution Process*
- **Presentation Details**: Megan Mesko and Erin Meredith provided insight into why funders may decide to allow costs questioned by external auditors. The presentaiton team also included the associate director of financial compliance at a not-for-profit organization and the director of Contacts & Grants Accounting at the University of California-Davis.

ACUA

- **Presentation Title:** *Congratulations, You've Been Selected for an NSF Incurred Cost Audit!*
- **Presentation Details:** Megan Mesko provided insight into how internal audit can help prepare for a successful external audit outcome. The presentation team also included a member of Oregon State University's (OSU's) internal audit team who had completed an NSF incurred-cost audit at OSU.

SRAI

- **Presentation Title:** *Surviving an NSF Audit: How to Develop a Strategy and Plan for a Successful Audit*
- **Presentation Details:** Darwin Emmanuel, a supervisory senior on Cotton & Company's CGL team, assisted two members of the University of Connecticut's sponsored program service team in presenting this topic. Mr. Emmanuel had just completed a successful audit at the university, and the program service team requested that he provide his insight and input.

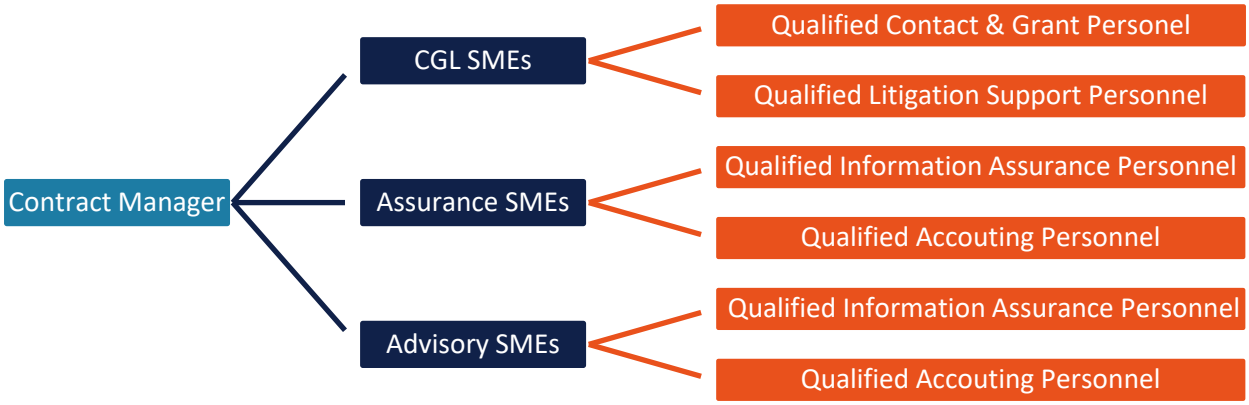
- ***Monitors Information, Analyses, and Advice Published by Recipients of Federal Funds.*** To ensure we are aware of emerging trends and topics of interest in the higher education community, Cotton & Company reviews articles, memoranda, and other materials published by the Council on Governmental Relations (COGR) and the Federal Demonstration Partnership (FDP). In addition to providing information on emerging trends and topics of interest, COGR and FDP both regularly publish guidance on best practices and provide resources to help their members in the areas of research administration and compliance, financial oversight, and intellectual property.
- ***Reviews Audit Resolution Reports.*** Because agency management does not always sustain the costs questioned in OIG audit reports, Cotton & Company continuously monitors management decisions on audits of IHEs to ensure we understand why the agency did or did not sustain a finding. This understanding ensures we can effectively identify and communicate future findings; it also provides us with insight into areas in which IHEs struggle to comply with relevant policies.
- ***Examines OIG Audit Plans.*** As part of their annual reporting process, most OIG offices publish an annual work plan that can be used to identify high-risk and other areas that the agency is potentially interested in examining during the upcoming year. We use these work plans to tailor our proposals and audit practices, enabling us to focus on emerging high-risk areas and other trending areas of interest.

4.a.6. Administering the Engagement [RFP Section XIII, Paragraph B.4.a.6. Describe your process for working with Mason's Office of Audit, Risk, and Compliance to administer the overall engagement.]

To deliver this engagement in a manner consistent with our industry-leading principles of quality and integrity, we will implement an effective contract management plan. Our contract manager, Ms. Mesko, has previously overseen similar contracts for co-sourcing services, and she will work with both Mason's Office of Audit, Risk, and Compliance and Cotton & Company SMEs to ensure that Cotton & Company:

- Assigns qualified personnel to each engagement.
- Engages in consistent, frequent communication and coordination with all relevant Mason contact(s).
- Appropriately monitors and communicates project status (including key milestones, tasks, risks, issues, deliverables, budgets, and scheduling conflicts).

Cotton & Company ensures that we appropriately staff each task order to achieve its unique objectives by focusing on strong project management principles and outstanding communication. By centralizing project management, we will be able to ensure that we assign appropriate SMEs and qualified staff to each task order, maintain strong control over the engagement process, and ensure effective communication. The following figure illustrates our centralized project management team:



4.a.6.a. Personnel Capability and Qualifications [RFP Section XIII, Paragraph B.4.a.6.a. Describe the individuals likely to administer and provide overall oversight to the engagement. Provide resumes.]

We have assembled a team of highly qualified, highly skilled, and well-respected professionals with strong financial and compliance audit backgrounds that can be available to provide the requested co-sourcing services. Although we tailor our staffing plans based on each engagement's unique objectives, we have included brief highlights of eight employees to represent the proficiencies that Cotton & Company personnel in each experience category will provide. We have included these individuals' resumes in **Appendix A: Personnel Resumes**.

Experience Level	Cotton & Company Personnel
1–3 Years	[redacted]
1–3 Years [IT Specialty]	
3–5 Years	
>5 Years	
Manager	
Manager/ Subject Matter Expert (SME) [IT Specialty]	
In-Depth Subject Matter Expert (SME)	Megan Mesko, CPA, CFE
In-Depth Subject Matter Expert (SME) [IT Specialty]	[redacted]

Cotton & Company's workforce includes a diverse set of skilled professionals that includes Certified Public Accountants (CPAs), Certified Internal Auditors (CIAs), Certified Fraud Examiners (CFEs), Certified Information Systems Security Professionals (CISSPs), Certified Information Systems Auditors (CISAs), Certified Government Financial Managers (CGFMs), and many others, all of whom are well qualified to provide independent and objective risk-based assurance and consulting services.

[redacted], ***Staff.*** [redacted] joined Cotton & Company in January 2021 after graduating from the University of Central Florida, where he worked as an accounting assistant in the Office of Sponsored Programs in the College of Community Innovation & Education. As an accounting assistant, [redacted] created invoices and recorded revenue on facility rentals, as well as budgeted and booked travel plans for faculty. [redacted] also ensured the correct charges were filed to the correct accounts and departments, approved faculty members' purchases, and performed account transfers between departments to correct account balances and allocate funds within Oracle's PeopleSoft financial software.

[redacted], ***Senior [IT Specialty].*** [redacted] has participated in several technical performance audits on behalf of federal agencies, including participating in cybersecurity audits under FISMA legislation. [redacted]'s workstreams included testing configuration management and patch management of a federal agency's infrastructure. [redacted] also supported Cotton & Company's audit of advanced persistent threats of a federal agency; the audit included analysis of firewall rules and ingestion, indexing, analysis, and reporting of incidents in a SIEM system. [redacted] has also participated on an audit evaluating mobile device management tools and implementation, and he currently supports an audit evaluating the strategy, implementation, monitoring, and overall governance of the adoption of cloud-based technologies at a legislative-branch agency.

[redacted], ***Senior.*** [redacted] has performed audits of—and on behalf of—a number of federal and not-for-profit organizations. She has extensive experience performing audits and compliance reviews of contract and grant funding awarded to IHEs, hospitals, and not-for profit entities. In addition to performing external audit and review services, [redacted] has provided internal consulting services to both not-for-profit and for-profit organizations, including Mason. Specifically, during her time on site at Mason, [redacted] assisted with the annual audit preparation, the National Collegiate Athletic Association (NCAA) audit of Mason, and various other audit work, including conducting budgeting analytics for FY 2019 to plan for FY 2020 and completing various reconciliations.

[redacted], ***CIA, Senior.*** [redacted] gained more than 8 years of experience in auditing, accounting, finance, commercial operations, and retail banking for a large banking company. Most relevantly, she served as a staff auditor and conducted QA reviews on completed audits to assess engagement execution, coverage of key risks and controls, quality of workpaper documentation, and adherence to professional and departmental standards. These reviews focused on financial services, financial crimes, compliance, technology, credit card, and risk management audits. Specifically, [redacted] conducted interviews, performed follow-up inquiries, and articulated recommendations to audit teams; developed workpapers highlighting performance on all QA reviews; wrote draft audit reports based on exceptions identified from QA reviews; and communicated findings to the senior manager. [redacted] also performed QA reviews on annual risk assessments for entities within the organization, to ensure that potential risks were appropriately categorized; reviewed 25 percent of samples within the audit file to review testing of controls; researched applicable laws and regulations; compiled data and supporting documents; used analytical tools and processes to improve the effectiveness and efficiency of audit execution; and developed and implemented training material for six summer interns and eight new incoming staff auditors in the audit rotation program, ensuring the staff auditors had sufficient onboarding and preparation to begin performing audits.

[redacted], ***CPA, CFE, CGFM, Senior Manager.*** [redacted] has experience performing and managing compliance reviews, audits, and other attestation engagements of—and on behalf of—federal and non-profit organizations. She has performed examinations, performance audits, and compliance reviews of contract, grant, and other federal funds awarded to IHEs, hospitals, and not-for-profit entities. In addition to performing external audits and reviews, [redacted] has also provided consultative services for a non-profit organization. Her responsibilities have included developing and performing a risk assessment of the organization's award portfolio, assisting with the design and implementation of new internal/ external compliance activities, including the development of pre-award reviews, and determining whether contract expenses claimed by an awardee were supported and allowable for reimbursement at the time of the awardee's dissolution. [redacted] is familiar with Salesforce, SharePoint, PeopleSoft, Oracle, Banner, Intacct, IDEA, and other accounting systems and software.

[redacted], ***CISSP, CISA, Senior Manager [IT Specialty].*** [redacted] has performed IT audits at a number of IHEs and not-for-profit organizations, and he has extensive experience conducting IT audits at large financial services institutions. His experience at IHE and non-profit clients includes IT general control reviews, an enterprise resource planning pre-implementation assessment, and business continuity audits. Prior to joining Cotton & Company, [redacted] was a director in Capital One's internal audit department, where he led IT audits related to core technology, IT infrastructure, cloud, and customer-facing banking applications. He was primarily responsible for the execution of audits, including determining audit scope, developing test plans, reviewing workpapers, and providing reports to audit executives. [redacted] is the current Chairman of the Board of the Northern Virginia Chapter of the Institute of Internal Auditors, where he also has served as a past President of the chapter.

[redacted] ***CPA, CFE, Partner.*** [redacted] has managed and performed audits of—and on behalf of—a number of federal and not-for-profit organizations. She has extensive experience performing data analytics-focused audits and compliance reviews of contract and grant funding awarded to IHEs, hospitals, and not-for profit entities. In addition to performing external audit and review services, [redacted] has provided internal consulting services to both not-for-profit and for-profit organizations. These services have included performing risk assessments of an organization's award portfolio, assisting in the development of an organization's internal and external compliance monitoring programs, and providing consulting support services to ensure that grant expenses claimed by an organization were adequately supported and complied with relevant cost principles.

[redacted] ***CPA, CISSP, CISA, Partner [IT Specialty].*** [redacted] joined Cotton & Company in May 2002, and he was elected a partner in April 2003. [redacted] leads Cotton & Company's IT and security audit engagements, and he has more than 26 years of diversified information system audit, financial and operational audit, and risk management consulting experience. In particular, [redacted] has a long history of providing support to internal audit departments and IHEs. [redacted]'s IHE experience began in 1999, when he assisted Georgetown University in preparing for Y2K, and has continued for the past 20 years. His most recent IHE engagement involved assisting Mason's Assistant Controller in extracting and analyzing data from Banner to assist in the budget preparation processes. [redacted] is also a frequent presenter at conferences on the topics of IT auditing, cybersecurity, privacy, contingency planning, fraud, and internal controls.

Replacement of Personnel/Backup Personnel

Cotton & Company is well positioned to handle any vacancies that may arise during contract performance. Partners meet biweekly to discuss staff scheduling, which enables them to efficiently assign staff across multiple projects and quickly identify resource gaps on engagements. We have more than 180 full-time employees, including a full-time recruiter dedicated to placing the right people with our firm. We also have teaming agreements with a large number of subcontractors that have successfully teamed with us on other engagements and that we can quickly call upon to supplement our resources when necessary and in the best interest of our clients.

Cotton & Company also cross-trains staff members on our engagements, delegating primary and backup responsibilities to ensure our team always has the expertise necessary to perform mission-critical tasks. Additionally, team leads are responsible for directing and understanding the tasks under their supervision to the degree that they can perform the tasks as a backup, if necessary. Cross-training has proven successful in mitigating the risks of resource transition; however, it is also essential to our staff's growth, advancement, and job satisfaction. This provides staff with exposure to the overall engagement and enables them to both better understand and better contribute to the overall objectives and requirements of our clients and the government's financial management initiatives. When our teams make significant contributions, exceed client expectations, and obtain recognition for their achievements, it fosters a work environment that is rewarding and more stable.

Cotton & Company understands that there are circumstances under which employees may need to be replaced or removed without the ideal advance notice and transition planning. All resource assignments will be approved by Mason and executed in a manner that will result in minimal disruption or concern for the Office of Audit, Risk, and Compliance.

4.a.6.b. Invoicing and Payment Processes [RFP Section XIII, Paragraph B.4.a.6.b. Describe the Invoicing and payment processes.]

Cotton & Company will invoice all hours worked on a time-and-materials basis to Mason's Accounts Payable address, and we will accept Mason's Net 30 payment terms, consistent with Option #3 in the Request for Proposal. Each invoice will reference the corresponding Mason Purchase Order Number, Vendor Taxpayer ID Number, and details of goods/services, consistent with the original order.

Cotton & Company holds an active SWaM certification, is a registered vendor with eVA, and does not have any exceptions regarding Mason's standard contract and general terms and conditions.

4.a.6.c. Communication Channels to Coordinate and Manage the Project

Open lines of communication are the key to early identification and resolution of any problems that might surface. Internally, we require weekly routine reporting by all team members to the engagement manager, who then reports to the partner. Additionally, all team members are aware that they should immediately report to the engagement manager when problems arise. This process enables the manager to quickly evaluate the situation, assess its seriousness, and determine the appropriate action.

Cotton & Company is committed to establishing and maintaining open, responsive, frequent communication with agency management. We will follow instructions governing communication with agency personnel, attend status meetings, provide all written status reports on their due dates, and conduct entrance and exit conferences. We will notify agency management immediately if we identify problems or potential problems.

4.a.7. Sample Engagement Letters [RFP Section XIII, Paragraph B.4.a.7. Provide a sample engagement letter template likely to be used in this engagement.]

We have provided two example engagement letters based on the two scenarios that Mason identified in its response to Q&A #38: one letter that applies to scenario (i) and one letter that applies to scenario (ii). Please see **Appendix B: Sample Engagement Letters**.

4.a.8. References [RFP Section XIII, Paragraph B.4.a.8. Provide names, firms, and contact information for three (3) reference clients with whom you have had a successful working relationship.]

Cotton & Company is proud of our successful working relationships with our clients. We have provided point of contact (POC) information for three of our current projects that are most relevant to Mason's requested co-sourcing services.

Client Name	Architect of the Capitol (AOC) Office of Inspector General (OIG)
Project Title	Construction Audit Services
Date of Service	[redacted]
Point of Contact Name and Contact Information	[redacted]
Contract Value	[redacted]

Client Name	Patient-Centered Outcomes Research Institute (PCORI)
Project Title	Financial Management, Accounting, Policies and Procedures, Compliance and Reporting Support Services
Date of Service	[redacted]
Point of Contact Name and Contact Information	[redacted]
Contract Value	[redacted]

Client Name	Federal Deposit Insurance Corporation (FDIC)
Project Title	IT Audits, Evaluations, and Expert Services
Date of Service	[redacted]

	[redacted]
Point of Contact Name and Contact Information	[redacted]
Contract Value	[redacted]

5. COSTS [RFP SECTION XIII, PARAGRAPH B.5. COSTS]

Below, Cotton & Company has provided its proposed hourly labor rates by level of experience.

5.A. PROPOSED HOURLY LABOR RATES BY LEVEL OF EXPERIENCE [RFP SECTION XIII, PARAGRAPH B.5.A. PROVIDE HOURLY COSTS BY LEVEL OF EXPERIENCE (E.G., 1-3 YEARS, 3-5 YEARS, > 5 YEARS), AND SPECIALTY (E.G., OPERATIONAL, INFORMATION TECHNOLOGY)]

Cotton & Company will propose a total cost for each task order based on the proposed staff, staff availability, and the recommended SMEs using the following rate ranges, as negotiated with Mason:

Years of Experience	Non-IT Specialty		IT Specialty	
	Low* Range	High** Range	Low* Range	High** Range
1–3 Years	$85	$99	$85	$105
3–5 Years	110	130	110	135
>5 Years	140	170	140	175
Manager	175	225	170	200
In-Depth Subject Matter Expert (SME)	230	270	230	270

* Low – Just entered position (0–2 years in position, plus progressive audit experience leading up to the level)
** High – Long-term in position (2+ years in position, plus progressive audit experience leading up to the level) or a demonstrated set of highly specialized skills needed for engagement.

We will use this established rate structure for all variable hours-level internal audit and related work engagements to be completed under the overall direction of Mason's Office of Audit, Risk, and Compliance function.

Cotton & Company will provide future services in accordance with Mason's contractual requirements while maintaining compliance with our federal programs.

5.B. Volume Discounts [RFP Section XIII, Paragraph B.5.a. Provide information related to volume / discount breakpoints.]

Cotton & Company is pleased to provide discounts on the labor portions of time-and-materials and labor-hour orders that exceed prescribed thresholds, as follows:

- 0.5% discount – task order engagement amounts greater than $750,000
- 1.0% discount – task order engagement amounts greater than $1,250,000
- 1.5% discount – task order engagement amounts greater than $1,750,000
- 2.0% discount – task order engagement amounts greater than $2,250,000

Each order and each year of an order is treated as a separate and distinct price for discount calculation purposes. Should an order's labor dollar value be modified during performance, the savings realized by Mason through our proposed discounts will also be adjusted proportionally.

5.C. Travel and Other Direct Costs [RFP Section XIII, Paragraph B.5.b. Describe how you propose to handle any travel or out-of-pocket expenses related to provisions of these services. Specifically address expenses for resources based in locations near Mason.]

Cotton & Company's proposed rates are inclusive of all local travel and administrative overhead expenses. Accordingly, we will not bill Mason for travel or other direct costs unless specifically approved within a task order engagement.

6. INFORMATION PROTECTION [RFP SECTION XIII, PARAGRAPH B.6. *INFORMATION PROTECTION]*

Below, we provide information regarding Cotton & Company's information security measures.

6.A. Safeguarding Sensitive Information [RFP Section XIII, Paragraph B.6.a. Describe the protections you will use to safeguard information obtained during engagements from unauthorized use and disclosure, including, but not limited to, personal facts and circumstances related to individuals as well as information related to Mason's actual or anticipated business facts and circumstances.]

Cotton & Company is in compliance with FISMA, OMB Circular A-130, and NIST SPs and Federal Information Processing Standards (FIPS). We are aware of the sensitive nature of the information obtained during any of our engagements, and we take extreme care in protecting information obtained during the course of our work, including but not limited to, personal facts and circumstances related to individuals, as well as information related to Mason's actual or anticipated business facts and circumstances. Accordingly, our laptops are encrypted with FIPS 140-2-verified PGP whole-disk encryption. Cotton & Company laptops are thus only accessible to authorized personnel involved with the project, leveraging two-factor authentication. All systems are configured with the applicable U.S. Government Configuration Baseline and use common security configurations available from the NIST National Checklist Program Repository. Cotton & Company centrally manages and installs the Sophos Endpoint Antivirus product to provide real-time system protection. Signatures are checked automatically and updated daily. Additionally, we use Quest KACE to automatically manage the deployment of Microsoft and third-party patches.

Cotton & Company will coordinate with Mason, as determined necessary, in moving data to our locally housed servers to ensure proper protections are in place and data is compartmentalized appropriately. As our work typically involves more sensitive data, we are accustomed to potential access restrictions that could be in place.

Reporting Requirements/Incident Response

Cotton & Company has formal policies and procedures in place regarding incident response. Our goal is to create an atmosphere of vigilance and awareness regarding our responsibilities in protecting information. We consider any incident to be significant, including but not limited to data breaches (including PII breaches), security issues, or other related information security violations. We will immediately report all incidents or suspected incidents to appropriate Mason personnel.

Clearances

All Cotton & Company employees must be eligible to obtain a Top Secret or Secret clearance upon hire and must maintain that eligibility throughout their employment. Many of Cotton & Company's financial and IA personnel undergo the process of applying for Top Secret or Secret clearances, and many prospective employees begin the security clearance process prior to their hire date. Please see **Appendix A: Personnel Resumes** for our proposed personnel's clearance information.

Personnel receive an initial security briefing and a copy of the security manual upon joining the firm and undergo annual refresher courses thereafter. We also provide both monthly and ad hoc notifications regarding current security trends and issues.

APPENDIX A: PERSONNEL RESUMES

Megan Mesko
CPA, CFE
Partner

Years Experience
Cotton & Company 9.5

Education
B.S., Accounting & Information Systems and Finance, Virginia Tech, 2011

Certification
CPA: Virginia, 2012 (#39721)
CFE: 2014

CPE
2020: 25
2019: 85

Security Clearance
Top Secret: October 18, 2011

Ms. Mesko joined Cotton & Company in July 2011 and was elected a partner with the firm in January 2019. During her career, Ms. Mesko has performed a variety of audits and other reviews of government and non-profit grantees/contractors, with the majority of her experience consisting of performance audits and compliance reviews of costs claimed by institutes of higher education (IHEs), state or local governments, hospitals, and non-profit organizations. Her experience is highlighted below.

FINANCIAL AND PERFORMANCE AUDITS

National Science Foundation (NSF), Office of the Inspector General (OIG). *Senior*, February 2013 – July 2014; *Supervisory Senior,* July 2014 – January 2016; *Manager*, January 2016 – May 2018; *Senior Manager,* June – December 2018; *Partner*, January 1, 2019 – Present
Under the five-year (2014–2019) Blanket Purchase Agreement (BPA) to provide audit services for the NSF OIG, Ms. Mesko participated in 20 cost-incurred performance audits of NSF grant funds issued to 19 IHEs and one for-profit company. She was in charge of the team responsible for using IDEA software to detect and extract data anomalies in each organization's general ledger for further testing and for testing the extracted transactions to evaluate the allowability, allocability, and reasonableness of each transaction in accordance with relevant Federal criteria (including the Office of Management and Budget's [OMB] Code of Federal Regulations), NSF's *Proposal and Award Policies and Procedures Guide*, NSF award-specific terms and conditions, and organization-specific policies and procedures.

Under Cotton & Company's current five-year BPA with the NSF OIG, Ms. Mesko has performed, or is currently performing, seven audits at seven IHEs. Each of these audits involves a preliminary survey phase, the purpose of which is to evaluate the grantee's award management environment and to create an organizational risk assessment, which is used to determine whether any further audit testing should be performed. Ms. Mesko is in charge of the team that performs the organizational risk assessment (which includes evaluating the strengths and weaknesses of the organization's internal controls, testing a sample of judgmentally selected

transactions, and providing recommendations on areas to perform additional audit work) and expanded audit work (which could include a performance audit, an internal control audit, or an accounting system audit), as determined necessary.

Ms. Mesko also participated in two performance audits of management fees awarded under cooperative agreements (CAs) awarded by NSF. Specifically, in response to congressional inquiries made in 2014 regarding the use of management fees on NSF CAs, the NSF OIG hired Cotton & Company to (1) evaluate how the fees were awarded under each CA and (2) examine how the awardees recorded and expended the fees they received. Ms. Mesko was responsible for evaluating whether the management fee expenses were accumulated in compliance with the requirements established in the applicable CAs; whether the fees were necessary to facilitate the basic operations and viability of the awardees; and whether the fees were used to pay for allocable, reasonable and allowable expenses.

Corporation for National and Community Service (CNCS), OIG. *Staff, January – August* 2012; *Senior,* January – August 2013; *Supervisory Senior*, November 2014 – May 2015; *Manager*, November 2015 – May 2016; *Manager,* November 2017 – May 2018; *Senior Manager*, June – December 2018; *Partner*, January 1, 2019 – Present
Ms. Mesko has participated in five agreed-upon procedures (AUPs) of funding awarded to State Commissions. The objective of these AUP engagements is to determine whether CNCS-funded federal assistance provided to grantees was expended in accordance with grant terms and provisions, laws, and regulations, as well as to report upon compliance, controls, and questioned costs. Ms. Mesko has performed detailed member testing, other direct cost testing, living allowance testing, salary testing, and all other testing and reporting steps required for the completion of the AUPs.

In addition to auditing funding awarded to CNCS grantees, Ms. Mesko has also participated in the performance audit of CNCS's compliance with the Improper Payments Elimination and Recovery Act of 2010 (IPERA) for fiscal years (FY) 2014, 2015, 2017, 2018, and 2019. During these engagements, Ms. Mesko is responsible for reviewing the information that CNCS reports in its Annual Management Reports to evaluate whether it has complied with OMB's criteria for compliance with IPERA as described in OMB Memorandums M-15-02 and M-18-20. Specifically, Ms. Mesko is responsible for determining whether CNCS's payment population is complete, evaluates whether the attribute testing models are reasonable and comprehensive, and re-performs attribute testing to evaluate CNCS's conclusions regarding whether sampled transactions relate to proper or improper payments.

COMMERCIAL FINANCIAL CONSULTING ENGAGEMENTS

Patient-Centered Outcomes Research Institute (PCORI). *Manager,* July 2016 – May 2018; *Senior Manager*, June – December 2018; *Partner*, January 1, 2019 – Present
Ms. Mesko assisted in the development of—and is responsible for overseeing—risk assessments performed on PCORI's active research portfolio on an annual basis, which has involved reviewing more than 400 contracts representing more than $2.3 billion in funding that PCORI awarded to nonprofit organizations, IHEs, and for-profit organizations from 2016 through 2020.

Based on the results of these annual risk assessments, Ms. Mesko leads a team that identifies the high-risk organizations that will be selected for compliance reviews during the year and has lead 89 compliance reviews of contracts awarded to 53 different IHEs, hospitals, and non-profit research organizations. Each of these reviews involved reviewing the contract's specific terms and conditions, reconciling the contractor's accounting system records to costs it invoiced to PCORI, and selecting and testing a judgmental sample of transactions to ensure compliance with PCORI contract terms and conditions.

In addition to providing external compliance review services, Ms. Mesko also provides internal consulting services to PCORI to assist its Financial Compliance team develop its internal and external compliance monitoring programs and pre-award risk assessments.

New York University (NYU) Marron Institute. *Partner,* December 2019 – Present
Ms. Mesko participated in a consulting engagement to review expenditures that NYU Marron reported to the United Nations Office for Project Services (UNOPS) for costs accumulated under a contract it award to support a Climate Resilient Cities Project in Grenada. Ms. Mesko confirmed the receipt of UNOPS funding and examined award expenditures to evaluate whether expenses NYU charged to the contract had been incurred in accordance with NYU's policies and procedures, as well as the terms and conditions established within the UNOPS contract.

Virginia Department of Transportation (VDOT), Assurance and Compliance Office. *Manager*, May – June 2016
Ms. Mesko conducted a review of an audit over a consulting engineering firms' indirect cost rates. The audit under review was performed by a CPA firm in accordance with the American Association of State Highway and Transportation (AASHTO) *Uniform Audit and Accounting Guide for Audits of Architecture and Engineering Consulting Firms.* Ms. Mesko reviewed the CPA firm's workpapers to ensure compliance with generally accepted government auditing standards (GAGAS), generally accepted auditing standards (GAAS), Federal Acquisition Regulation (FAR) Part 31, AASHTO guidance, and other interpretive guidance and also determined whether the recommended indirect cost rates were in accordance with the FAR.

The National Museum of Natural History (NMNH) – Smithsonian Institution. *Supervisory Senior,* December 2014
Ms. Mesko participated in a consulting engagement to review expenditures that NMHH reported to the Charities Aid Foundation (CAF) for costs accumulated under its awards. Ms. Mesko confirmed the receipt of CAF contributions and examined award expenditures to evaluate whether the expenses appeared to have been incurred in accordance with the charitable aims and objectives of the NMNH.

Community Care Network of Virginia (CCNV). *Staff,* January – October 2012
Ms. Mesko participated in an engagement to perform consulting services at an organization that had received U.S. Department of Health and Human Services (HHS), Health Resources and Services Administration (HRSA) funding. The team provided consulting support to ensure expenses incurred by CCNV for five grants were adequately supported and complied with FAR

cost principles, as well as HRSA program requirements. Ms. Mesko analyzed expenditures for the five grants, which totaled over $4.3 million, to determine whether they were allowable under grant provisions and assisted in the development of the firm's indirect cost rate.

FINANCIAL STATEMENT AUDITS

Ms. Mesko has participated in a number of financial statement audit engagements, gaining experience in applying applicable OMB, Government Accountability Office (GAO), American Institute of Certified Public Accountants (AICPA), and International Financial Reporting Standards (IFRS) policies and requirements and ensuring financial audit requirements are met.

New York University (NYU) Marron Institute. *Manager,* August 2017 – April 2018
Ms. Mesko has performed two financial statement audits of single financial statements prepared in accordance with a special purpose framework under AICPA and IFRS standards. Ms. Mesko was responsible for identifying all applicable AICPA and IFRS standards applicable to the audit and ensuring that all applicable audit steps under these standards were completed.

She has also participated in the following financial statement audits under the Chief Financial Officers (CFO) Act in accordance with GAO/President's Council on Integrity and Efficiency's (PCIE's) *Financial Audit Manual* (FAM):

- ***U.S. Department of Justice (DOJ), United States Marshals Service (USMS).*** *Staff,* FY 2012. Ms. Mesko assisted the Information Assurance team with the IT portions of a federal financial statement audit. She participated in identifying and testing management, operational, and technical controls over financial systems using GAO's Federal Information System Controls Audit Manual (FISCAM) audit methodology. Ms. Mesko also gained experience in applying applicable OMB, GAO, and AICPA methodologies and requirements.
- ***U.S. House of Representatives, OIG.*** *Intern,* FY 2009. Ms. Mesko assisted in the planning phase of the audit. She conducted interviews and developed an understanding of various cycles within the House.

LITIGATION SUPPORT SERVICES

U.S. DOJ, Civil Division. *Staff,* September 2011 – December 2012. Cotton & Company assists in resolving litigation disputes before the U.S. Federal Claims Court and other adjudicators. Ms. Mesko has participated in the following engagements:

- ***Kellogg, Brown & Root.*** Ms. Mesko assisted in litigation support to the Defense Contract Management Agency (DCMA) on an Armed Services Board of Contract Appeals (ASBCA) case involving two Requests for Equitable Adjustment (REAs) for delay and double-handling allegedly incurred by a subcontractor in Iraq. The total amount of approximately $51 million was determined to be unreasonable by the government. Ms. Mesko assisted in determining whether the contractor met its burden of establishing that the costs claimed were reasonable and allowable, specifically focusing on the costs related to contractor-claimed delay days.
- ***Kellogg, Brown & Root.*** Ms. Mesko assisted in reviewing claims for costs, $42 million and $13.3 million respectively, initially determined to be unreasonable, incurred by a

subcontractor to provide dining facility services in Iraq. Cotton & Company reviewed the issue to determine whether the contractor met its burden of establishing that the costs claimed were reasonable and allowable.

Commercial Litigation Support and Consulting Engagements. Cotton & Company assists contractors with claim preparation and other support surrounding termination and equitable adjustment claims against the government. Ms. Mesko has participated in the following engagements:

- ***Southeastern Pennsylvania Transportation Authority (SEPTA) vs. Philadelphia Transit Consultants (PTC).*** *Intern,* June – July 2010; *Staff,* June – July 2011. Cotton & Company assisted in resolving a dispute between SEPTA and PTC regarding repair costs. Ms. Mesko assisted in evaluating the accumulation of historical costs incurred by SEPTA, calculating estimated future restoration costs, and calculating estimated future repair costs.
- ***Philadelphia Industrial Development Corporation (PIDC).*** *Intern,* June – July 2010. Ms. Mesko assisted with the calculation of claimed costs representing PIDC's damages resulting from improper government estimates provided during contract procurement.

[redacted]
CPA, CISSP, CISA
Partner

Years of Experience
Cotton & Company 18.5
Other Professional 8

Education
B.S., Accounting, Virginia Tech, 1994

Licensing/Certifications
Certified Public Accountant (CPA): Virginia, 2001 (#[redacted])
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)

Affiliations
American Institute of Certified Public Accountants (AICPA)
Information System Audit and Control Association District of Columbia Chapter (ISACA)

CPE
2020: 50
2019: 31

Security Clearance
Top Secret: January 29, 2019

[redacted] has more than 26 years of diversified information system audit, financial and operational audit, and risk management consulting experience. He joined Cotton & Company in May 2002 and was elected a partner in April 2003. [redacted]'s experience includes directing and participating in a wide range of system reviews, Federal Information Security Modernization Act (FISMA) audits, financial statement audits, process reengineering improvement projects, and audits of internal management controls of automated information systems.

PERFORMANCE AUDITS

Library of Congress (LOC), Copyright Modernization Audit. *Partner*, October 2018 – August 2019
[redacted] led an engagement to conduct a performance audit of LOC's information technology (IT) modernization project for the Copyright Recordation System. The scope of the engagement included evaluating the U.S. Copyright Office's (USCO's) and Office of the Chief Information Officer's (OCIO's) compliance with LOC's system development life cycle (SDLC) and project management life cycle (PMLC) policies and directives and determining whether the IT modernization project was on schedule and within budget. The engagement also included a review and analysis of the Contracting Officer's Representative (COR) function and role in USCO's Copyright Modernization project.

Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG). *IA Partner,* July 2016 – Present
[redacted] has led engagements to assist the FDIC OIG in conducting performance audits of the following FDIC programs and applications:

- **Audit of Microsoft Windows Active Directory,** 2020. [redacted] is leading an engagement to assist the FDIC OIG in determining whether the FDIC has designed and implemented effective controls and processes for AD to protect network systems and data.
- **Audit of Mobile Device Security and Management,** 2019. [redacted] is leading an engagement to assist the FDIC OIG in assessing whether the FDIC has established and implemented controls to effectively manage and secure its mobile devices, including Apple iPhones and Apple iPads.

- **Regional Automated Document Distribution and Imaging System (RADD),** 2018. [redacted] led an engagement to assist the FDIC OIG in performing an audit of security controls over RADD. The work included assessing the effectiveness of selected security controls designed to protect the confidentiality, integrity, and availability of information.
- **Advanced Persistent Threats,** 2017. [redacted] led an audit of the FDIC's ability to detect and respond to advanced persistent threats. The audit involved reviewing the configurations and related processes for firewalls and the FDIC's Security Incident and Event Management tool.
- **Security of the OIG's Email Vault,** 2016. [redacted] led an engagement to perform audit services in support of a project to increase the security of the FDIC OIG's email vault. The audit included performing a search to identify any misdirected emails, determining what caused the emails to be misdirected, and making recommendations regarding how to prevent future items from being incorrectly routed.

National Archives and Records Administration (NARA) Wireless Audit. *QC Partner*, 2014
The engagement included analyzing the existing wireless environment, determining the scope of the audit, developing the audit work program, and performing the associated testing. This review focused on NIST 800-97 security recommendations and applicable NIST 800-53 control areas.

External-Facing Information Technology Audit for the Internal Audit Department, Frederick County, Maryland. *QC Partner*, 2013
This audit focused on evaluating information security controls over Frederick Community College's (FCC's) remote access, patch, and vulnerability management processes; configuration of external-facing firewalls; and controls over public and private wireless access points. Audit procedures included detailed reviews of FCC's documented policy, procedure, and security configuration documentation for compliance with industry best practice, as well as interviews with key personnel. Technical testing carried out included reviewing external-facing firewall rulesets and conducting external vulnerability and wireless scanning.

FISMA AUDITS AND REVIEWS

[redacted] leads independent information security (IS) evaluations for compliance with FISMA, *Government Auditing Standards*, AICPA standards for consulting services, and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*. Work includes preparing or assisting the agency in preparing the Inspector General's segment of the FISMA independent evaluation report and template for submission to OMB. Specifically, [redacted] has directed and participated in audits of the following federal agencies:

- **Federal Deposit Insurance Corporation.** *Partner,* 2015 – Present
- **Board of Governors for the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB).** *Partner,* Fiscal Year (FY) 2020 – Present
- **Export-Import Bank of the U.S. (EXIM).** *Partner*, FY 2008; *Quality Control (QC) Partner*, FYs 2009 – 2011, 2013 – 2017
- **U.S. Agency for International Development (USAID).** *QC Partner*, FYs 2013 – 2014
- **Overseas Private Investment Corporation.** *QC Partner*, FY 2013

- **National Gallery of Art (NGA).** *Partner*, FYs 2008 – 2012
- **DOJ.** Each component was awarded as a separate task order. Each team assessed the component's compliance with both federal and DOJ privacy requirements by interviewing key privacy personnel, reviewing privacy policies and procedures, and assessing the quality of privacy impact assessments conducted on major applications.
  - **Environment and Natural Resources Division.** *QC Partner*, FY 2016
  - **Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).** *Partner*, FYs 2008, 2010, and 2012
  - **Justice Management Division (JMD).** *Partner*, FYs 2009 – 2012
  - **Civil Division.** *Partner*, FY 2012
  - **Executive Office of the U.S. Trustees (EOUST).** *Partner*, FY 2012
  - **Tax Division.** *Partner*, FY 2011
  - **Bureau of Prisons (BOP).** *QC Partner*, FY 2009
  - **U.S. Marshals Services (USMS).** *Partner*, FY 2009
- **Smithsonian Institution.** *Partner,* FYs 2006 – 2009
- **Department of Health and Human Services (HHS).** *Partner*, FY 2007
- **U.S. International Trade Commission (ITC).** *Partner*, FYs 2005 – 2006
- **National Credit Union Administration.** *Partner*, FYs 2003 – 2005

FINANCIAL STATEMENT AUDITS

[redacted] has directed and participated in the IT portions of federal financial statement audit engagements. He is experienced in applying applicable OMB, GAO, and AICPA methodologies and requirements and ensuring that IT audit teams meet all audit requirements. [redacted] directed the IT portions of financial statement audits, which involve full FISCAM audits, of the following federal agencies:

- **U.S. Transportation Command, Transportation Working Capital Fund.** FYs 2018 – Present
- **Defense Health Program, Air Force Medical Service (AFMS).** FY 2019 – Present
- **GAO Schedule of the Federal Debt Audit.** FY 2006 – Present
- **GAO FDIC.** FY 2013 – Present
- **GAO Consumer Financial Protection Bureau (CFPB).** FYs 2013 – 2018
- **GAO Federal Housing Finance Agency.** FYs 2013 – 2016
- **U.S. House of Representatives.** FYs 2004 – 2009; 2012 – 2017
- **U.S. Navy, Audit of the General Fund Schedule of Budgetary Activity.** FY 2015
- **Architect of the Capitol.** FYs 2013 – 2014
- **U.S. Department of Justice (DOJ), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).** FYs 2010 – 2011
- **United States Capitol Police (USCP).** FYs 2002 – 2010
- **DOJ, U.S. Marshals Service (USMS).** FYs 2004 – 2009
- **Congressional Budget Office (CBO).** FY 2008
- **U.S. Equal Employment Opportunity Commission.** FYs 2003 – 2008, *Manager* (preaudit), FY 2002
- **Defense Nuclear Facilities Safety Board.** FYs 2004 – 2007
- **GAO.** FYs 2004 – 2005

FEDERAL IT CONSULTING ENGAGEMENTS

U.S. Department of Education (ED), OMB Circular A-123 IT Assessment. *Partner,* 2015 – Present
Cotton & Company is assisting ED in conducting an IT assessment in accordance with OMB Circular A-123, Management's Responsibility for Internal Control, and Appendix A of OMB Circular A-123, Internal Control over Financial Reporting. Specifically, Cotton & Company is performing a risk analysis of internal controls over the Education Central Automated Processing System (EDCAPS) General Computer Controls (GCC). The team is updating the IT risk assessment, IT rotation plan, GCC planning and scoping memo, control matrix, and test plans and developing exceptions, observations, and recommendations.

Pension Benefit Guaranty Corporation (PBGC), OMB Circular A-123 Services. *Partner,* 2013 – 2017
[redacted] assisted in providing PBGC with OMB Circular A-123 services. The team performed reviews for general support systems and financial systems based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. These reviews focused on critical control sets. Based on the results of these reviews, [redacted] provided detailed recommendations to management to address identified issues. He also performed remediation testing when appropriate. In addition, [redacted] taught classes for PBGC covering topics that included controls and governance.

Department of Defense, Army, Quality Control Reviews. *QC Partner,* FYs 2013 – 2014
As a subcontractor to KGS, [redacted] performed quality control reviews on FISCAM audit reports for an engagement to provide the U.S. Medical Command (MEDCOM) with audit support services. [redacted] also directed the firm's team. The engagement included documenting information system controls for core financial feeder systems for each MEDCOM activity to determine whether the controls were in place and operating to protect the confidentiality, integrity, and availability of data.

Securities and Exchange Commission (SEC), OMB Circular A-123, Appendix A Implementation. *IA Partner,* 2010
[redacted] managed an engagement for the Office of the Executive Director to identify, document, and test controls over financial reporting in accordance with OMB Circular A-123, Appendix A. The team assisted SEC in establishing a management control structure, providing Appendix A training to SEC personnel, and performing planning tasks to identify significant reports, accounts, business processes, and locations. They also documented key general and application-level information system controls and related business processes. In addition, the team tested key controls to determine design and operational effectiveness, assisted in development and implementation of corrective action plans, and provided input regarding the appropriate annual statement of assurance.

[redacted] led the IT portion of SEC's implementation of OMB Circular A-123. The work products from [redacted]'s team were heavily relied upon by SEC's independent auditor and also contributed to the remediation of the Risk Assessment and Monitoring significant deficiency identified in the FY 2009 financial statement audit.

General Services Administration (GSA), Certification and Accreditation Reviews. *IA Partner,* 2008 – 2010

[redacted] performed and documented certification and accreditation (C&A) reviews for four major GSA systems. He managed the C&A process for Pegasys, GSA's core financial system, and its major applications. [redacted] wrote portions of system security plans (SSPs) and privacy impact assessments. He also assisted in a second C&A review for another system. This engagement was conducted under guidance from FISMA, GSA Procedural Guides, Federal Information Processing Standards (FIPS), and NIST Special Publications.

GSA, OMB Circular A-123 Services. *IA Partner,* FYs 2006 – 2010

[redacted] directed the IT portions of OMB Circular A-123 review consulting engagements. He was responsible for all aspects of this work, including developing audit procedures, assuring adequacy of all work performed, and advising team members as needed. Work addressed NIST SP 800-53 controls, including access management, audit and accountability, identification and authentication, system and information integrity controls, and system and services acquisition controls for 14 distinct applications that derive GSA's financial statements.

PRIVACY AUDITS AND REVIEWS

Smithsonian Institution. *Partner*, 2008

[redacted] led an engagement to audit privacy policies, procedures, and practices following federal and industry best practices. The team developed and administered a survey to key personnel to gain an understanding of where privacy data were being collected, processed, stored, and disseminated to identify controls in place over the data. The team conducted several after-hour walkthroughs of offices to determine whether sensitive privacy data in hard-copy format were being adequately protected.

U.S. Federal Election Commission (FEC). *Partner*, 2008

[redacted] conducted a privacy audit under requirements outlined in Section 522 of the 2005 Consolidated Appropriations Act. He assessed FEC policies, procedures, and practices for identifying and protecting identifiable information in electronic and hardcopy formats.

Federal Housing Finance Board (FHFB). *Partner*, 2006 and 2008

[redacted] conducted an engagement to review the adequacy of privacy and data protection policies, procedures, and practices. The engagement objectives were to determine compliance with privacy requirements in the 2005 Omnibus Bill, review practices and procedures regarding personal information, and make recommendations to improve policies, practices, and procedures over protecting personal information. [redacted] also conducted a detailed analysis of the intranet, network, and websites for privacy vulnerabilities, including noncompliance with stated policies, practices, procedures, and risks for inadvertent release of information in an identifiable form from the website.

U.S. Equal Employment Opportunity Commission (EEOC). *Partner*, 2008

[redacted] conducted this engagement under requirements outlined in the E-Government Act of 2002 and OMB memorandums. The team assessed EEOC policies, procedures, and practices for

identifying and protecting information in identifiable form both in electronic and hardcopy formats.

COMMERCIAL IT CONSULTING

Landon IP. *Security Authorization/Annual Assessment,* 2014 – 2017
[redacted] directed engagements to provide independent security assessment services for Landon IP's Security Authorization/Annual Assessment. The team performed testing on a subset of NIST SP 800-53 security controls for a U.S. Patent and Trademark Office (USPTO)-interfacing application. This work involved determining the extent to which controls were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements for the information system.

Landon IP. *System Security Plan Review Services*, 2014
[redacted] directed a separate engagement to provide policy, procedure, and SSP review services for Landon IP. The team ensured that IT policies and procedures were consistent and that the Landon IP Information System (LIPIS) SSP was consistent with IT policy and procedure requirements. The team also ensured IT policies and procedures and the LIPIS SSP reflected the processes in place and generally aligned with industry best practices and NIST requirements.

Other Commercial IT Consulting.
In addition to his work with Landon IP, [redacted] directed engagements to provide Sarbanes-Oxley (SOX) 404 compliance consulting for IT operations for two companies. Under his direction, the teams for these engagements assisted company management in identifying and documenting necessary policies and controls and performed management's internal testing and assessment of controls.

COMMERCIAL IT ATTESTATION ENGAGEMENTS

Captricity, Inc. Service Organization Control (SOC) 2 Type II Report. *Engagement Partner*, 2015
Cotton & Company was engaged to provide an independent attestation over the design and effectiveness of controls related to trust principles defined by the AICPA. The engagement focused on examining and reporting on the description of the service organization's system and the suitability of the design and operating effectiveness of system controls relevant to security, availability, process integrity, confidentiality, and privacy, using the trust services criteria. The engagement culminated with delivery of a SOC 2 Type II report.

SPEAKING ENGAGEMENTS

[redacted] has conducted speaking engagements for well-known organizations, including:

- Center for Fraud Prevention and Detection, on the topic of OMB Circular A-123 compliance, with a second speaking engagement on the topic of identity theft.
- Association of Government Accountants, Montgomery County Chapter, on the topic of privacy impact assessments.
- Small Agency CIO Council, on the topic of FISMA.

- Baltimore Association of Government Auditors and the Institute of Internal Auditors (IIA)'s Government Accounting and Audit Conference, on the federal implications of the Sarbanes-Oxley Act.
- The Virginia Society of Certified Public Accountants (VSCPA), on the topics of:
    - What All CPAs Should Know About Information Technology
    - Identity theft
    - Extensible Business Reporting Language (XBRL), an open specification that uses XML-based data tags to describe financial statements for both public and private companies
    - The DC IIA conference, on the topic of privacy issues.
    - The IIA DC Chapter, on the topic of FISMA.
    - The ISACA DC Chapter, on the topics of identity theft and contingency planning.
    - The Federal Reserve System Conference on Auditor Development on topics such as contingency planning, application controls auditing, and project management for auditors.

[redacted]

CPA, CFE, CGFM

Manager

Years Experience

Cotton & Company 5

Other Professional 2.5

Education

B.S., Accounting, Salisbury University, Salisbury, MD, 2013

Licensing/Certifications

Certified Public Accountant (CPA): MD, 2015 (#[redacted]); VA, 2016 (#[redacted])

Certified Fraud Examiner (CFE)

Certified Government Financial Manager (CGFM)

Affiliations

Virginia Society of CPAs (VSCPA)

Association of Certified Fraud Examiners (ACFE)

Association of Government Accountants (AGA)

- Certificate of Excellence in Accountability Reporting (CEAR) Program 2015–2017

Greater Washington Society of CPAs (GWSCPA)

- Chair of the Government Auditing and Accounting Section 2017–2019

CPE

2020: 116.4

2019: 73

Security Clearance

In progress

[redacted] joined Cotton & Company in January 2016 with 2.5 years of professional experience in accounting, auditing, and finance. Her professional experience is detailed below.

Financial and Performance Audits

National Science Foundation (NSF), Office of the Inspector General (OIG). *Senior* Manager, October 2020 – Present; *Manager*, January 2019 – September 2020; *Supervisory Senior*, January 2017 – December 2018; *Senior*, January 2016 – December 2017

[redacted] is participating in cost-incurred performance audits of NSF grant funds issued to universities, each of which involves a preliminary survey phase that leads to a recommendation for whether a performance, internal control, or accounting system audit should be performed.

[redacted] is responsible for managing the team that reviews each organization's policies and procedures to evaluate strengths and weaknesses of its internal controls, selects and tests a sample of transactions, and provides recommendations to the NSF OIG regarding whether any additional audit work may be appropriate. She uses IDEA software to detect and extract data anomalies in each organization's general ledger for further testing.

[redacted]'s responsibilities include reviewing tested extracted transactions to evaluate the allowability, allocability, and reasonableness of each transaction in accordance with 2 Code of Federal Regulations (CFR) 220 (formally OMB *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*), NSF allowability criteria, and organization-specific policies and procedures; reviewing original award documents, award modification requests, approval documents, and correspondence between NSF and the auditee to determine whether expenses appear to be reasonable and appropriately approved; examining the results of the initial testing sample; and evaluating which data tests should be expanded to identify additional anomalies within organizational data.

[redacted] is currently participating in audits of universities' implementation of the temporary Coronavirus Disease 2019 (COVID-19) administrative flexibilities issued by OMB and the related NSF implementation guidance.

[redacted] is responsible for managing the team that is conducting walkthroughs and obtaining an understanding of how awardees used NSF and other funding (e.g. Higher Education Emergency Relief Funds, Paycheck Protection Program) to cover costs; reviewing and reconciling awardee financial data to expenses claimed in the Award Cash Management $ervice; and using data analytics to judgmentally test expenses incurred in accordance with the COVID-19 flexibilities to determine whether the chosen expenses are allowable, allocable, and reasonable.

[redacted] is also participating in a performance audit of an institution awarded Established Program to Stimulate Competitive Research (EPSCoR) grants, the focus of which is evaluate whether costs claimed are supported, allowable, allocable, reasonable, and in compliance with NSF award terms and conditions and federal requirements. Procedures are generally the same as those described for the cost-incurred performance audits noted above, with an increased focus on cost-sharing, subaward expenditures, and costs typically unallowable on EPSCoR awards.

Corporation for National and Community Service (CNCS). *Senior Manager*, October 2020 – Present; *Manager*, January 2019 – September 2020; *Supervisory Senior,* July – December 2018 [redacted] is currently assisting the CNCS OIG on two investigations regarding false claims for funding awarded to two State Commissions and their subawardees, in accordance with the Council of Inspectors General for Integrity and Efficiency (CIGIE) *Quality of Standards for Federal Offices of Inspector General*. [redacted] is responsible for reviewing documentation provided by the CNCS OIG and State Commissions to validate the number of ineligible education awards, calculate questionable and fraudulent timesheet hours, quantify questioned costs for funds expended by the State Commissions, and summarize potential false claims and associated monetary damages. She is also responsible for attending meetings with personnel from the CNCS OIG and United States Attorney's Office to discuss findings and preparing documentation to present the findings, as requested.

[redacted] participated in an agreed-upon procedures engagement of funding awarded to one State Commission. The objective was to determine whether CNCS-funded federal assistance provided to the grantee was expended in accordance with grant terms and provisions, laws, and regulations, and to report upon compliance, controls, and questioned costs. [redacted]'s responsibilities included supervising the work of others; participating in fieldwork, including a site visit at grantee and subgrantee locations and performing member and other direct cost testing; and preparing reports with recommendations to address compliance and internal weaknesses found within the grantee and subgrantee grant administration environment

[redacted] also participated in a limited-scope performance audit of federal assistance funds awarded to a subawardee of one State Commission. The objective of this engagement was to determine whether the subawardee's Education Award Only members for two program years were eligible to be AmeriCorps members, and whether appropriate National Service Criminal History Checks were completed for eligible members. Based on information obtained during the planning phase of this audit, the issues identified were escalated within the CNCS OIG. The audit engagement was terminated, and the OIG is now conducting an investigation of these programs, as described above.

Library of Congress (LOC), OIG. *Supervisory Senior,* August 2017 – September 2018
Cotton & Company assisted the LOC OIG with a variety of performance audits related to the procurement process, as well as provided support on investigations. [redacted] participated on an investigation of information technology (IT) contracts procured, awarded, and administered by LOC's Copyright Office. She was responsible for reviewing bid and solicitation documents, researching individuals at the awarding agency and winning contractors, and evaluating any instances of potential collusion or misconduct. [redacted] also participated in performance audits of 11 contracts across various service units within LOC. Specifically, she reviewed procurement and award documentation to determine whether the award was appropriately procured and administered, and tested extracted transactions to evaluate the allowability, allocability, and reasonableness of each transaction in accordance with LOC and other applicable federal regulations. [redacted] used Momentum software, LOC's financial system of record, and the Invoice Processing Platform (IPP), to select payment transactions for testing.

The National Air and Space Museum (NASM) – Smithsonian Institution. *Manager,* June 2019 – October 2020
[redacted] participated in an attestation compliance examination of surcharge funds expended related to sales of the U.S. Mint's 2019 Apollo 11 50th Anniversary Commemorative Coin. [redacted] was responsible for examining management's assertion related to NASM's Schedule of Surcharge Funds Received and Expended. This included conducting discussions with management and obtaining an understanding of the Destination Moon Exhibit, internal controls, and financial reporting; completing reconciliations; identifying risk and materiality as it relates to the subject matter; performing tests of expenditures incurred, as reported on the Schedule of Surcharge Funds Received and Expended; and creating the practitioner's report for the examination engagement. Previously [redacted] participated in an attestation compliance audit of donations raised. This included auditing NASM's Schedule of Funds Raised from Private Sources by confirming the receipt of funds raised from private sources.

Previously [redacted] participated in an attestation compliance audit of donations raised. This included auditing NASM's Schedule of Funds Raised from Private Sources by confirming the receipt of funds raised from private sources.

Universal Service Administrative Company (USAC) – Internal Audit Division. *Senior*, June – October 2016
Under two 3-year contracts with USAC, Cotton & Company performed an assessment program designed by USAC and the Federal Communications Commission (FCC) to determine estimated rates of improper payments for the Universal Service Fund (USF) programs, in accordance with Generally Accepted Government Auditing Standards (GAGAS). Each year, Cotton & Company selects and tests samples of more than 1,000 expenditures to ensure the accuracy of USAC payments to program applicants. [redacted] assisted in performing site visits, which included assessing specific payments made to selected beneficiaries to determine if the payments were made in accordance with FCC rules.

COMMERCIAL FINANCIAL CONSULTING ENGAGEMENTS

Patient Centered Outcomes Research Institute (PCORI). *Senior Manager*, October 2020 – Present; *Manager*, January 2019 – September 2020; *Supervisor Senior*, January 2017 – December 2018; *Senior*, July 2016 – December 2017

[redacted] assisted in the development of criteria used to perform a risk assessment applied to contracts and awards representing more than $2.3 billion in funding across more than 400 contracts that PCORI awarded to nonprofit organizations, colleges and universities, for-profit organizations, and national associations from 2016 through 2020. Based on the results of this risk assessment, the team has conducted desk reviews for 108 contracts and awards at 60 different universities, hospitals, and non-profit organizations. The reviews involve testing a judgmental sample of transactions to ensure compliance with PCORI contract terms and conditions and organizational policies. [redacted] is responsible for reviewing contract terms and conditions, contract modifications, guidelines issued by PCORI, and the policies of the organization to determine whether the tested expenses are appropriate. [redacted] has also conducted site visits at 15 of these organizations to discuss relevant policies and procedures, interview staff, and review documentation made available at the awardee's location.

[redacted] is also providing consultative services for the design and implementation of new compliance activities at PCORI, including PCORI's internal compliance review program and externally-performed pre-award reviews. She is responsible for creating checklists, process guides, flow-charts, workpapers, and other templated reports to design, develop, and implement the compliance activities. This work involves interviewing relevant PCORI personnel to incorporate feedback into the design of each activity and incorporate feedback to refine compliance activities; providing recommendations regarding how to address observations and financial risks identified; and presenting recommendations to the Chief Operating Officer and other PCORI leadership.

[redacted] provided consultative services to assist PCORI in closing six agreements awarded under a Master Infrastructure Funding Contract held with an organization that dissolved in Fiscal Year 2020. [redacted] managed the team that was responsible for determining whether all general ledger information provided by the organization supported expenses reimbursed by PCORI; evaluating whether advanced payments provided by PCORI were utilized for allowable project expenses; determining whether indirect costs were charged and used in accordance with the organization's proposals and indirect cost rate agreements; and presenting relevant financial information to PCORI executives and General Counsel throughout the dissolution process.

FINANCIAL STATEMENT AUDITS

Center for Folklife and Cultural Heritage (CFCH) – Smithsonian Institution. *Manager,* March – June 2019

[redacted] performed a financial statement audit of a single financial statement prepared in accordance with a special purpose framework under American Institute of Certified Public Accountants (AICPA) standards. [redacted] was responsible for identifying all AICPA standards applicable to audits of single financial statements prepared in accordance with a special purpose framework and ensuring that all applicable audit steps under these standards were completed.

PREVIOUS PROFESSIONAL EXPERIENCE

Chortek LLP **August 2013 – December 2015**

Senior Accountant/Auditor (December 2014 – December 2015)

As a senior accountant/auditor with a firm providing accounting, auditing, and tax compliance services, [redacted]

- Trained staff on required audit procedures and Prosystem software applications.
- Participated in federal financial statement audits, performing procedures in areas such as Fund Balance with Treasury, Budgetary Resources, Obligations Incurred, Operating Expenses/Program Costs, Payroll and Benefits, and compliance with laws and regulations.
- Participated in cost-incurred performance audits of federal grant funds awarded to various entities nationwide; reviewed grant agreements, communicated with awardees, and used data analytics to evaluate data provided by grantees.
- Tested transactions to ensure compliance with the Uniform Grant Guidance issued by OMB, as well as with the provisions of the grant agreement. Tests included ensuring that grant funds were not used for unallowable costs, verifying that indirect costs were billed using the correct rate, and verifying that expenditures were incurred consistently with the agreed-upon budget.
- Provided non-profit and federal agencies with consulting services such as financial management support, data analytics, organization of database information, and assistance with annual audits.
- Developed formal financial management policies and procedures and contracting guidelines for two federal government agencies. These documents outlined personnel responsibilities and described steps to be taken for key functions.
- Conducted internal control assessments and made recommendations to management regarding actions to strengthen internal controls within the agency.

Staff Accountant/Auditor (August 2013 – December 2014)

- Performed analytical and substantive testing on four audits of executive-branch agencies.
- Provided financial management consulting services to an educational non-profit organization.
- Helped prepare and submit Congressional budget testimonies, summaries of performance and financial information, and Annual Financial Reports for specialized agencies.
- Performed compilation and review services for federal agencies.

Naval Air Systems Command **July 2010 – January 2013**

Co-op Accountant

As a GS-05-01 under the Comptroller's Accounting Division for the Naval Air Systems Command (NAVAIR) program, [redacted]

- Assisted in audit readiness projects under the Financial Improvement Audit Readiness (FIAR) initiative. Tasks included compiling transaction information from the database to provide to auditors, responding to inquiries about accounting practices, and completing questionnaires provided by auditors.
- Recorded inventory and maintained a log of assets for an office of approximately 50 employees.
- Researched outstanding contract issues to identify options for resolution; evaluated the remaining level of funding on certain contracts and identified amounts requiring de-obligation.
- Managed enterprise resource planning (ERP) database information for the Department of the Navy and performed review transactions.

[redacted]

CISA, CISSP, CRMA

Senior Manager

Years Experience

Cotton & Company <1
Previous Professional 17

Education

M.S., Cybersecurity Technology, University of Maryland Global Campus, expected 2021
B.S., Computer Engineering, University of Florida, 2003

Licensing/Certifications

Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Certification in Risk Management Assurance (CRMA)

Affiliations

Institute of Internal Auditors (IIA), Northern Virginia Chapter (Chairman)

CPE

2020: 51
2019: 48.5

[redacted] joined Cotton & Company as a senior manager in November 2020. He has 17 years of experience predominately in the financial services industry as an audit practitioner, consultant, and information technology (IT) analyst. He has in-depth experience leading technology, business-integrated IT, and Sarbanes-Oxley (SOX) audits.

[redacted] volunteers his time for the Northern Virginia Chapter of the Institute of Internal Auditors, where he currently serves as Chairman of the Board and has previously served as chapter President and Vice President.

Since joining Cotton & Company, [redacted] has participated in several internal projects, including the CMMC certification project. His experience is detailed below.

Previous Professional Experience

Capital One **February 2017 – August 2019**
Director, Technology Audit

- Led a book of technology audits composed of core technology, infrastructure, and emerging technology (e.g., cloud) for the following organizational capabilities: Customer-Facing Banking Applications, Customer Identity Management, Third-Party Data Sharing, API Gateway, Data Center and Platform Management, Access Management, and Network Operations.
- Owned book of staff operations audits that included Human Resource Operations, Compensation, and Corporate Governance.
- Oversaw team of approximately 20 IT audit professionals, including 10 direct reports.
- Directed execution of audits using a risk-based approach by providing guidance on audit scope during planning, developing test plans, reviewing workpapers, and providing quality reports to audit executives.
- Developed the annual audit plan by performing risk assessments, creating the audit schedule, setting audit budgets, and staffing audits.

- Built and maintained relationships with key executives across various lines of business, including Digital, Enterprise Services, Risk Management, Compliance, Legal, and Human Resources.
- Developed summary excerpts of high-risk issues to support quarterly Board reporting.
- Performed audit issues trending analysis to provide insight to senior executives on the risk, nature, and prevalence of audit issues identified during the quarter.
- Led departmental diversity and inclusion efforts by establishing relationships with professional associations, organizing recruiting events, and driving internal initiatives.

Protiviti, Inc. **January 2014 – January 2017**
Associate Director/Senior Manager, Internal Audit/IT Consulting

- Planned, led, and executed IT audits and IT consulting projects in the following areas: IT SOX, IT Integrated Audits, Business Continuity & Disaster Recovery, Pre-Implementation Project Reviews, E-Commerce, IT Governance, End User Computing, GLBA, IT Vendor Management, IT Security Policies, Payment Card Industry (PCI), and Firewall Management.
- Wrote reports for client management that identified deficiencies and provided both tactical and strategic recommendations to mitigate risk.
- Managed multiple client engagements concurrently while supervising multiple staff consultants, ensuring quality project deliverables, and meeting strict deadlines.

Manager, Internal Audit and Financial Advisory/IT Consulting *January 2012 – December 2013*

- Led and executed IT audits and IT consulting projects.
- Managed project administration tasks (e.g., project setup, project budget, billing, revenue recognition).
- Conducted interviews of potential IT audit and IT security consultants.

Senior Consultant, Internal Audit and Financial Advisory *September 2010 – December 2011*

- Led and executed IT SOX and IT audit testing efforts for a variety of client engagements with limited supervision.
- Presented audit recommendations to client management.
- Drafted and reviewed audit reports.
- Led UNIX security training sessions for new and experienced consultants.

Society for Worldwide Interbank Financial Telecommunication **May 2006 – September 2010**
Associate Technology Auditor

- Led and executed IT SDLC/Project and Business Continuity audits.

- Executed IT audits in the following areas: Product Acceptance and Certification, Change Management, Problem and Incident Management, Facility Management, and Software Development Life Cycle (SDLC).
- Assisted lead IT auditor by identifying risks and formulating risk and control matrices.
- Prepared business overviews and detailed test plans.
- Created and executed test plans for Statement on Auditing Standards (SAS) 70 controls on an annual basis in the following areas: Encryption, Acceptance and Certification, and Business Continuity.
- Assisted lead IT auditors with performing annual risk assessments and auditing planning.

Gannett Co., Inc. **May 2004 – May 2006**
IT Auditor *March 2005 – May 2006*
IT Specialist *May 2004 – March 2005*

[redacted]
CIA
Senior

Years Experience
Cotton & Company 1.5
Previous Professional 8

Education
M.S., Accounting, University of Maryland College Park, 2017
B.S., Accounting, Hampton University, 2008

Licensing/Certifications
Certified Internal Auditor (CIA)

CPE
2020: 103
2019: 66.5

Security Clearance
Secret: January 31, 2020

[redacted] joined Cotton & Company in September 2019 as a senior with previous auditing experience. Her experience is highlighted below.

Financial and Performance Audits

Universal Service Administrative Company (USAC), Internal Audit Division. Senior, 2019 – Present

[redacted] conducts performance audits for USAC's Internal Audit Division in its examination of recipients of Universal Service Fund (USF) Schools and Libraries Program (SLP) funds related to disbursements from USF for a 12-month period. She continuously performs fieldwork and reviews of the schools and libraries' required filings for compliance with relevant regulations for USF SLP support. With customer service being of high priority, [redacted] effectively communicates inquiries with school representatives throughout the audit. In addition, she adheres to USAC policies as they relate to the handling of confidential data, documents, and correspondences.

Previous Professional Experience

Capital One **September 2010 – September 2018**

Serving in positions of increasing responsibility, [redacted] gained more than 8 years of experience in auditing, accounting, finance, commercial operations, and retail banking for a large banking company. Most relevantly, she served as a staff auditor and conducted quality assurance (QA) reviews on completed audits to assess engagement execution, coverage of key risks and controls, work paper documentation quality, and adherence to professional and departmental standards. Reviews focused on Financial Services, Financial Crimes, Compliance, Technology, Credit Card, and Risk Management audits. Specifically, [redacted] conducted interviews, follow-ups, and articulated recommendations to audit teams; developed working papers highlighting performance on all QA reviews; and wrote draft audit reports based on exceptions identified from QA reviews and communicated findings to the Senior Manager.

In addition, [redacted] performed quality assurance reviews on annual risk assessments for entities within the organization, to ensure that potential risks were appropriately categorized; reviewed 25 percent of samples

within audit file to review testing of controls; researched applicable laws and regulations; compiled data and supporting documents; utilized analytical tools and processes to improve the effectiveness and efficiency of audit execution; and developed and implemented training material for six summer interns and eight new incoming Staff Auditors in the Audit Rotation Program, ensuring onboarding and proper preparation to begin performing audits.

[redacted]

Senior

Years Experience
Cotton & Company 3.5

Education
B.S., Accounting and Information Systems, Virginia Tech, 2017

CPE
2020: 46.5
2019: 36.5

Security Clearance
Secret: June 20, 2017

[redacted] joined Cotton & Company in July 2017 as a staff auditor after obtaining her undergraduate degree. Her experience is highlighted below.

FINANCIAL AND PERFORMANCE AUDITS

George Mason University (Mason). *Senior,* January 2020 – [redacted] assisted Mason's Finance Department with various audit activities and financial analytical support during a 3-week onsite engagement. These activities included supporting Mason's annual audit preparation and assisting with the National Collegiate Athletic Association (NCAA) audit of Mason. Specifically, [redacted] conducted budgeting analytics for fiscal year (FY) 2019 to plan for FY 2020; she also completed various reconciliations.

National Science Foundation (NSF), Office of Inspector General (OIG). *Senior,* October 2019 – Present; *Staff*, July – September 2019
[redacted] has participated in nine cost-incurred performance audits of NSF grant funds issued to various universities. She performs testing in accordance with 2 Code of Federal Regulations (CFR) 220 (formerly Office of Management and Budget [OMB] Circular A-21), the Uniform Guidance (2 CFR 200), NSF allowability criteria, and university-specific policies and procedures to determine each transaction's allowability. She also assists in performing data analytics and sample selection for the audits, as well as reviews transactions sampled from the universities' financial systems to identify and report on instances of non-compliance with regulations, federal financial assistance requirements, and the provisions of the NSF award agreements as they relate to the transactions tested. [redacted] has also conducted cluster testing on transactions.

[redacted] is also currently participating in two engagements that involve gaining an understanding of a university's implementation of various flexibilities granted by the Office of Management and Budget (OMB) in response to the Coronavirus Disease 2019 (COVID-19) pandemic. [redacted] is part of the team conducting interviews to evaluate whether—and how—universities have implemented the COVID-19 flexibilities, using a data analytics approach to

conduct judgmental testing of expenses incurred in accordance with the flexibilities. She also evaluates whether the universities' implementation of these flexibilities conforms to applicable federal guidance and NSF terms and conditions.

COMMERCIAL FINANCIAL CONSULTING ENGAGEMENTS

Patient-Centered Outcomes Research Institute (PCORI). *Staff,* September 2018 – Present
[redacted] has participated in dozens of compliance reviews of PCORI contract funds issued to universities, hospitals, and not-for-profit organizations. These reviews include developing an understanding of the organization's policies and procedures, reconciling awardee financial records to costs invoiced to PCORI, and testing whether expenses charged to the award are compliant with PCORI's contract terms and conditions. [redacted] has participated in each step of these compliance reviews, including selecting judgmental sample of transactions to test and writing final reports that include recommendations regarding how contracted organizations can improve their controls to ensure future compliance with contract terms and conditions.

[redacted] has also previously assisted PCORI in designing and implementing financial compliance activities, including:

- Verifying contract values recorded in PCORI's financial database(s) were correct.
- Identifying the causes of any discrepancies identified.
- Updating contract data in PCORI's financial database(s), as necessary.
- Performing tests and reviews of the year-end accrual preparation.
- Performing other accrual clean-up activities as requested by PCORI's finance team.

FINANCIAL STATEMENT AUDITS

U.S. Transportation Command (USTRANSCOM), Audit of the Working Capital Fund (WCF). *Staff,* July 2017 – August 2018
Cotton & Company is performing an audit in accordance with generally accepted auditing standards (GAAS); the standards applicable to financial audits contained in *Government Auditing Standards* (GAS), issued by the Comptroller General of the United States; and applicable sections of OMB Bulletin 15-02, *Audit Requirements for Federal Financial Statements*, to determine whether USTRANSCOM's FY 2018 WCF financial statements and related notes were fairly presented, in all material respects, in accordance with generally accepted accounting principles (GAAP), as promulgated by the Federal Accounting Standards Advisory Board (FASAB).

[redacted] worked on the Property, Plant, and Equipment (PP&E) and Revenue and Receivables teams, where she was responsible for:

- Performing non-sampling control testing, including observations, inquiries, walkthroughs, and inspection of documentary evidence over USTRANSCOM's control activities to assess the design and implementation of key internal controls over financial reporting.

- Designing population reconciliation schedules for re-performing USTRANSCOM's populations and validations of key general ledger accounting systems to the reported amounts in the financial statements.
- Assisting in developing tests and procedures in conducting interviews and site visits.
- Performing dual-purpose testing of balances of the financial statements, including Earned Revenue, Accounts Receivable, Filled and Unfilled Customer Orders, and Collections.
- Assessing the sufficiency and accuracy of key Revenue and Receivables reconciliations and processes.

PREVIOUS PROFESSIONAL EXPERIENCE

Collins & Company, CPAs **Summer 2015**

Tax Intern

As a tax intern with a CPA firm, [redacted]

- Prepared individual income tax returns using QuickBooks and other accounting software.
- Observed and assisted in tax planning, preparation, and consulting services for a variety of entities.
- Researched tax law changes to ensure clients received appropriate recommendations for tax savings.

Sturdy Savings Bank and Financial Services **Summer 2016**

Summer Banking Intern

As an intern with a financial institution, [redacted] served as a bank teller, sat in on meetings with clients, and assisted in analyzing finances.

[redacted]

Staff

Years Experience

Cotton & Company Newly hired
Previous Professional 1

Education

B.S.B.A., Accounting, University of Central Florida, 2020

CPE

Due to his hire date in January 2021, [redacted]'s first full CPE period will include CYs 2021 and 2022.

[redacted] joined Cotton & Company in January 2021 with 1 year of previous professional experience. His experience is detailed below.

Financial and Performance Audits

National Science Foundation (NSF), Office of Inspector General (OIG). *Staff Auditor*, January 2021 to Present

[redacted] is currently participating in audits of universities' implementation of the temporary Coronavirus Disease 2019 (COVID-19) administrative flexibilities issued by OMB and the related NSF implementation guidance. He is also participating in a performance audit of an institution awarded Established Program to Stimulate Competitive Research (EPSCoR) grants, the focus of which is evaluate whether costs claimed are supported, allowable, allocable, reasonable, and in compliance with NSF award terms and conditions and federal requirements. [redacted] prepares audit workpapers and tests transactions for various universities and grant recipients.

Previous Professional Experience

University of Central Florida
September 2019 – December 2020
OPS Student Accounting Assistant – Budgeting

[redacted] created invoices and recorded revenue on facility rentals, as well as budgeted and booked travel plans for faculty. He also ensured the correct charges were filed to the correct accounts and departments, approved faculty members' purchases, and performed account transfers between departments to correct account balances and allocate funds.

Reality Marketing Group, LLC
September – December 2018
Sales Intern

[redacted] created sales plans, performed cold calls, and sent outgoing emails to further develop the company's client base. He also assisted with the creative marketing plans and price quotes for various clients.

OTHER EXPERIENCE

[redacted] also has experience as a golf specialist for a sporting goods store, where he sold and fit customers for golf clubs, as well as performed any club maintenance or repairs. In this role, he also performed cashier duties and general retail customer service.

As an attendant at a resort and golf club, [redacted] assisted members with their clubs, cleaned carts, and tended to the golf range. He also helped organize tournaments and golf outings for members.

APPENDIX B: SAMPLE ENGAGEMENT LETTERS

635 Slaters Lane, 4th Floor | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

[Date]

[Contact Name]
[Contact Title]
George Mason University
4400 University Drive
[Secondary Address]

Subject: Internal Audit Co-Sourcing Services, [Applicable Request]

This letter confirms our understanding that George Mason University (Mason) requires a [Years of Experience/ Position] to augment its team of auditors under the direct supervision of [Relevant University Auditor] from [Period of Performance].

Based on discussions with the [Relevant University Auditor], Cotton & Company will provide an experienced [Years of Experience/Position], [Cotton & Company Employee Name], who has the specialized knowledge and expertise required to assist Mason's audit team.

Based on the anticipated timeline for these co-sourcing services and the rates established within [Relevant Contract], the estimated cost to complete this engagement is [Estimated Cost], as follows:

Consultative Services Estimated Costs				
Years of Experience/Position	**Name**	**Rate**	**Hours**	**Cost**
Total Estimated Costs				

Mason shall pay Cotton & Company all reasonable expenses up to [Estimated Cost] for all services required under this engagement letter on a time-and-materials basis, as set forth within [Relevant Contract]. Mason shall not be obligated to pay any additional amounts for the services set forth in this engagement letter. Cotton & Company shall notify Mason in writing when we have expended 80 percent of the budget amount and as soon as we anticipate any need for additional funding.

Cotton & Company will submit invoices for work performed under this amendment under on a monthly basis with payment of undisputed amounts due to Cotton & Company net [No.] days, as outlined within [Relevant Contract].

We shall consider all documentation and information provided to or prepared by us while working on this engagement to be proprietary and confidential, and we shall not release it to outside parties without your express written permission.

If the foregoing is in accordance with your understanding, please sign and return to us one copy of this letter.

I look forward to continuing our relationship.

_____	_____
Megan Mesko, CPA, CFE	Date

Accepted:

_____	_____
[Name, Title]	Date

635 Slaters Lane, 4th Floor | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

[Date]

[Contact Name]
[Contact Title]
George Mason University
4400 University Drive
[Secondary Address]

Subject: Internal Audit Co-Sourcing Services, [Applicable Request]

This letter confirms our understanding of the terms and objectives of our engagement to provide [Requested Services] in accordance with the Statement on Standards for Consulting Services promulgated by the American Institute of Certified Public Accountants (AICPA) and [Any Other Relevant Standards]. I will be the partner-in-charge of all consulting services provided, and I will call upon additional members of the firm to perform the reviews as deemed necessary.

We understand that George Mason University (Mason) requires [Requested Service Details]. To satisfy the requirements of this engagement, Cotton & Company will:

- Obtain [Relevant Documentation].
- Review and summarize [Relevant Information].
- Perform [Relevant Testing Procedures].
- Prepare [Relevant Summaries and/or Reports].
- Provide [Engagement Deliverables].

The anticipated period of performance for this engagement is [Period of Performance], and the key milestone dates for this engagement include:

- Entrance Conference:
- [Other Relevant Milestones]:
- Draft Report Deliverable:
- Final Report Deliverable:

The estimated cost to complete this engagement is [Estimated Cost], estimated as follows:

Consultative Services Estimated Costs				
Years of Experience/Position	**Name**	**Rate**	**Hours**	**Cost**
Total Estimated Costs				

Mason shall pay Cotton & Company all reasonable expenses up to [Estimated Cost] for all services required under this engagement letter on a time-and-materials basis, as set forth within [Relevant Contract]. Mason shall not be obligated to pay any additional amounts for the services set forth in this engagement letter. Cotton & Company shall notify Mason in writing when we have expended 80 percent of the budget amount and as soon as we anticipate any need for additional funding.

Cotton & Company will submit invoices for work performed under this amendment on a monthly basis with payment of undisputed amounts due to Cotton & Company net [No.] days, as outlined within [Relevant Contract].

We shall consider all documentation and information provided to or prepared by us while working on this engagement to be proprietary and confidential, and we shall not release it to outside parties without your express written permission.

If the foregoing is in accordance with your understanding, please sign and return to us one copy of this letter.

I look forward to continuing our relationship.

_____ _____

Megan Mesko, CPA, CFE Date

Accepted:

_____ _____

[Name, Title] Date