U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

November 1, 2022

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Dear Ms. Countryman:

The U.S. Chamber of Commerce ("the Chamber") writes regarding the Securities and Exchange Commission's (the Commission) proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Proposed Rule). The Chamber appreciates the additional opportunity to comment.

As the Chamber previously warned, the speed at which the Commission has been seeking to push through a huge volume of proposals has risked depriving even the Commission's own staff of the time needed to develop thoughtful, properly tailored rule proposals. The Chamber's warnings have borne out. The Commission recently reported that its own systems have been unable even to *capture* all of the public comments the Commission has received,[1] let alone facilitate a thorough review of those comments. Ironically, the rule in question – the cybersecurity disclosure rule – would mandate public companies to disclose certain cyber incidents within four days of those events occurring; yet in the case of the SEC's "technical glitch," the SEC is only now informing the public of a major technological problem that has plagued its internet comment form for at least 18 months. This delay in identification and reporting of the problem reflects a clear failure of internal processes within the SEC.

The Commission's Inspector General has identified other difficulties still. In a report attached as Exhibit A, the Inspector General highlighted concerns from managers in numerous SEC divisions that the Commission's "more aggressive [rulemaking] agenda" has "limit[ed] the time available for staff research and

[1] [1] See Resubmission of Comments, 87 Fed. Reg. 63,016, 63,016 (Oct. 18, 2022).

analysis."[2] The staff has not "received as much feedback during the rulemaking process, either as a result of shortened timelines during the drafting process or because of shortened public comment periods."[3] The staff is also shorthanded, and thus has been "relying on detailees, in some cases with little or no experience in rulemaking."[4] The Commission should proceed at a more manageable pace that ensures stakeholders are able to provide the input the Commission needs, and which gives the Commission the time it requires to do its important job properly.

In addition, please see for the Commission's consideration the attached letter signed by 34 industry and trade representative organizations on the Commission's Proposed Rule.

The Chamber again appreciates the Commission's decision to reopen the commenting window. The Chamber and its members remain ready to assist the Commission on this important issue.

Sincerely,

Tom Quaadman
Executive Vice President
Center for Capital Markets Competitiveness
U.S. Chamber of Commerce

---

[2] The Inspector General's Statement on the SEC's Management and Performance Challenges 3 (Oct. 13, 2022), https://www.sec.gov/files/inspector-generals-statement-sec-mgmt-and-perf-challenges-october-2022.pdf.

[3] *Id.*

[4] *Id.*

June 22, 2022

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Dear Ms. Countryman:

Our organizations, which represent sectors across the U.S. economy, write to provide input on the Securities and Exchange Commission's proposed rules on *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.

Collectively, our associations appreciate the goals of the SEC's proposed rules, which focus on increasing investors' knowledge of publicly traded companies' cybersecurity postures. We agree with Chair Gensler's view that "[a] lot of issuers already provide cybersecurity disclosure to investors" and that "companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."

However, the SEC's proposed reporting regime departs significantly from the Commission's 2018 interpretive guidance, which effectively balances investor interests with companies' cybersecurity disclosure obligations. The proposed rules could result in undermining cybersecurity by forcing companies to disclose incident information prior to the mitigation of vulnerabilities. Detailed public disclosures could give cybercriminals and state-backed hackers a trove of data to further victimize companies, harm law enforcement investigations, and disrupt public-private responses to cyberattacks. Also, the costs of the rulemaking outweigh its benefits to investors. Simply put, the proposed rules go too far and would place companies at heightened risk by compelling them to prematurely disclose increased amounts of cybersecurity incident information.

Many in the business community strongly believe that the Commission's proposal should not be finalized in its current form. Calibrating the rulemaking correctly requires the SEC to proceed with caution and coordinate with other parts of the federal government. Given the complexity of the proposal, as well as its impact on U.S. economic security and cybersecurity, the Commission should allow more time for industry input.

While this list is not exhaustive of our groups' views, we urge the Commission to consider the following points as it seeks to develop a cybersecurity incident and risk management disclosure regime that both informs investors and protects companies against malicious actors.

- **The disclosure of cybersecurity incidents should accommodate temporary delays for law enforcement and/or ongoing investigations.** The Commission's proposed rules need to be revised so that companies can temporarily delay reporting on material cybersecurity incidents because of law enforcement and/or ongoing national security investigations against illicit hackers where U.S. cybersecurity is at stake. Instead of undercutting industry-government cooperation, the SEC should urge companies to work with law enforcement and national security agencies to mitigate the impacts of cyber incidents and help bolster companies' security and financial positions, which would benefit investors.

  More specifically, all 50 U.S. states have passed laws authorizing delayed disclosures to consumers of breaches of their sensitive personal data to avoid compromising an ongoing law enforcement investigation. The Gramm-Leach-Bliley Act similarly authorizes such delayed disclosure by financial institutions, and federal law enforcement agencies make such requests of registrants in appropriate circumstances. Without a corresponding law enforcement exception, the proposed rules would undermine the judgment of the states and several federal agencies that law enforcement protects the public first.

  The Commission's proposed rules should enable companies to delay disclosures due to active investigations by law enforcement and other reasonable requests (e.g., to remediate a cybersecurity incident) like other state and federal reporting laws. Companies need time to conduct internal investigations to accurately determine an incident's true scope and impact. The proposed rules could easily compel companies to make premature disclosures driven more by compliance timelines than genuine cybersecurity incident remediation factors. Companies are rightly concerned that SEC requirements mandating them to report incident and vulnerability information too early could place them at greater risk.

  Further, hasty reporting may not necessarily be accurate, given the little time afforded to companies to report material cybersecurity incidents. It is possible that the severity of incidents could be overstated, thus having a potentially negative effect on a company's earnings.

- **The rulemaking should not override laws and regulations related to cybersecurity and protected disclosures.** The Commission's proposal overwhelmingly conflicts with the policy goals established by Congress in recent cybersecurity legislation, especially the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which was signed into law on March 15—less than a week after the SEC announced its cybersecurity proposal. The new law requires certain critical infrastructure entities to report on a confidential and protected basis covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. Congress intended CISA to be the primary entity for reporting cybersecurity incidents to the federal government. Lawmakers also said that a business should only have to report to federal agencies once.

Congress has explicitly emphasized the importance of protecting cybersecurity incident data from unwarranted disclosures. For companies that perform work for the Department of Defense (DoD), the SEC's proposed rules neither recognize nor align with the evolving cybersecurity standards and disclosures required of these contractors. Several years ago, DoD initiated a Cybersecurity Maturity Model Certification (CMMC) program for contractors that seeks to leverage existing standards associated with the National Institute of Standards and Technology (NIST) Special Publication 800-171 to protect controlled unclassified information in nonfederal systems and organizations. The SEC does not appear to consider the potentially contradictory, unnecessarily duplicative, or financially burdensome nature of its proposed rules when compared with the CMMC requirements.

Requirements under the CMMC process are evolving as DoD continues to adjudicate industry comments regarding its September 2020 interim rule, while working to publish another interim rule in early 2023. The CMMC process holds companies to a higher standard of cybersecurity than what is required of government agencies. The Commission appears to do the same with its proposed rules, which contributes to an imbalance of public- and private-sector responsibilities.*

Congress also clarified that vulnerability information should be coordinated based on principles consistent with international standards and leading industry practices requiring protection and strict confidence.

- **The practicality and value of disclosing "aggregate" cybersecurity incidents are unclear.** The proposed rules would require a company to disclose when a series of previously undisclosed cybersecurity incidents become material in the aggregate. The Commission's proposal is notably vague about when a number of individual cybersecurity incidents—taken together—would be considered materially reportable. Only in hindsight and with considerable business and government effort can some hacking campaigns be grouped together. The Commission does not seem to consider the costs and the difficulty of identifying and tracking material incidents in the aggregate. The feasibility and value of aggregate reporting to investors is questionable.

- **The unprecedented micromanagement of companies' cybersecurity programs is misguided and would not necessarily protect investors.** The proposed rules embody an unnecessary micromanagement pertaining to the composition and functioning of both the management and the boards of companies. The SEC should not insert itself via disclosure rules into how a company would design its plans to detect, respond to, and recover from cyber incidents. The proposed rules could put companies in jeopardy by forcing them to allocate resources toward compliance-based reporting rather than triaging the complex elements of identifying and resolving cybersecurity incidents. If shared prematurely, the

* Additional federal laws and regulations that mandate the protection of cybersecurity-related information include the Chemical Facilities Anti-Terrorism Standards program, the Critical Infrastructure Protection Reliability Standards program, the Health Insurance Portability and Accountability Act of 1996, and the Maritime Transportation Security Act of 2002.

public disclosure of vulnerability data could give attackers a roadmap to exploit reporting registrants.

Similarly, disclosing the finer points of a company's cybersecurity policies and processes is excessive. This requirement would make the registrant an attractive target for malicious actors that could acquire unwarranted insights into a company's practices and develop a game plan for future exploitation. A cybersecurity program reflects a company's tailoring of the relevant laws, regulations, and standards that fit its unique structure and business environment. The proposed governance disclosures, moreover, take a detailed, one-size-fits-all approach, which implies "best practices" that would not make operational sense to each company.

- **Agencies, including the SEC, need to prioritize streamlining reporting regulations.** The SEC's proposed rules leave businesses in the unfavorable position of facing conflicting cybersecurity reporting directives from several government entities. There needs to be more assertive streamlining of cybersecurity incident reporting policies to enable businesses to understand and follow clear and consistent guidelines and requirements. CIRCIA calls on the national cyber director (NCD) to lead an intergovernmental Cyber Incident Reporting Council composed of the Office of Management and Budget, CISA, and sector risk management agencies "to coordinate, deconflict, and harmonize" federal incident reporting requirements, including those issued through regulations. Considering CIRCIA, the SEC should collaborate with other federal agencies and cybersecurity policymakers, including the NCD, to both coordinate its proposed rules with other authorities and determine whether its requirements are advisable as written.

- **Company boards should prioritize managing cyber risks but not through SEC mandates requiring cybersecurity "expertise."** Our associations advocate for companies to proactively prioritize cyber risk management activities, but they are concerned about the SEC's call for companies to disclose the name of any board member who has cybersecurity expertise. We believe that board experts should not proliferate via government directives. Prescriptive disclosures intended to drive company behavior regarding which subject-matter experts sit on companies' governing bodies could lead to unwieldy and unwanted outcomes (e.g., giving investors a false sense of confidence because of the presence of a board cybersecurity "expert").

  Also, cybersecurity talent is scarce globally. It is unclear where companies would get the cybersecurity experts that would be driven by the Commission's proposed requirement to disclosure such expertise. There is a well-established lack of cybersecurity talent for the public and private sectors that would impede companies' abilities to recruit board cybersecurity experts. The SEC's proposal could even create unintended barriers for historically underrepresented groups to move into cybersecurity management or board leadership roles—not due to the lack of qualifications but to the absence of formal credentials (e.g., owing to their costs) and other certifications. Even if companies could obtain the relevant cybersecurity experts for board positions, no evidence has been

convincingly shown that this requirement would inform investors or improve companies' cybersecurity preparedness.

It is unlikely that even organizations such as NIST could readily pinpoint what constitutes expertise or experience in cybersecurity that would earn widespread agreement among industry professionals. Advancements in cybersecurity occur rapidly. Overseeing internal and external experts who are current in the field is more valuable than directors having outdated credentials. The SEC should accommodate a broader array of experiences than what the proposed rules' list of cybersecurity expert criteria encompasses. Consider Item 407's definition of an audit committee financial expert. It indicates, for example, that while a chief executive officer may not simultaneously serve as the company's accountant, this person may serve as an audit committee financial expert on the board because he or she has experience overseeing the accounting function at the company. Likewise, a suitable board cybersecurity expert may come from company management and not have formal schooling or training, but this individual understands cybersecurity practices and/or has experience supervising the company's personnel who are engaged in cybersecurity activities.

- **The term "cybersecurity incident" should be narrowed to correspond with significant incidents that do actual harm and existing definitions.** The scope of the SEC's definition of a cybersecurity incident is overly expansive. It should not be "construed broadly," as the Commission suggests. For reasons of consistency, agencies should avoid defining terms through their own processes. A reportable cybersecurity incident should track more closely with a "covered cyber incident" in CIRCIA or *Presidential Policy Directive, United States Cyber Incident Coordination* (PPD 41). PPD 41 refers to a "significant cyber incident" as a cyber incident that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." Material cybersecurity disclosures should correspond to significant incidents that do actual harm.

  In addition, companies need clarity in reporting requirements, which should be targeted to clear, objective criteria in any rule that the SEC—with industry input—develops. The definition of a cybersecurity incident, as currently written, would lead to the overreporting of cybersecurity incidents and not serve investors' decision making well.

Our organizations support responsible and protected cybersecurity reporting to the government, consumers, and investors, but we oppose the SEC's proposed rules as written. The proposal runs counter to sound cybersecurity policies and practices. It should be revised to better balance transparency with cybersecurity. We are ready to work with the Commission to develop a rulemaking that provides timely information to investors while mitigating risks associated with disclosing sensitive cybersecurity information to the public.

Sincerely,

ACA Connects—America's Communications Association
ACT | The App Association
Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance for Automotive Innovation
American Chemistry Council (ACC)
American Council of Engineering Companies (ACEC)
American Council of Life Insurers (ACLI)
American Fuel and Petrochemical Manufacturers (AFPM)
American Gas Association (AGA)
American Petroleum Institute (API)
American Property Casualty Insurance Association (APCIA)
Biotechnology Innovation Organization (BIO)
Competitive Carriers Association (CCA)
Consumer Technology Association (CTA)
CTIA
Federation of American Hospitals
The Fertilizer Institute (TFI)
Global Business Alliance
Healthcare Information and Management Systems Society (HIMSS)
Information Technology Industry Council (ITI)
Interstate Natural Gas Association of America (INGAA)
National Association of Broadcasters
National Association of Mutual Insurance Companies (NAMIC)
National Association of Chemical Distributors (NACD)
NCTA—The Internet & Television Association
National Electrical Manufacturers Association (NEMA)
NTCA—The Rural Broadband Association
Professional Services Council (PSC)
Securities Industry and Financial Markets Association (SIFMA)
Semiconductor Industry Association (SIA)
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce
USTelecom—The Broadband Association

Exhibit A

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

October 13, 2022

TO: Gary Gensler, Chair

FROM: Nicholas Padilla, Jr., Acting Inspector General

SUBJECT: *The Inspector General's Statement on the SEC's Management and Performance Challenges, October 2022*

The Reports Consolidation Act of 2000 requires the U.S. Securities and Exchange Commission's (SEC or agency) Office of Inspector General to identify and report annually on the most serious management and performance challenges facing the SEC.[1] In deciding whether to identify an area as a challenge, we consider its significance in relation to the SEC's mission; its susceptibility to fraud, waste, and abuse; and the SEC's progress in addressing the challenge. We compiled the attached statement on the basis of our past and ongoing audit, evaluation, investigation, and review work; our knowledge of the SEC's programs and operations; and information from the U.S. Government Accountability Office and SEC management and staff. We reviewed the agency's response to prior years' statements, and assessed its efforts to address recommendations for corrective action related to persistent challenges. We previously provided a draft of this statement to SEC officials and considered all comments received when finalizing the statement. As we begin fiscal year 2023, we again identified the following as areas where the SEC faces management and performance challenges to varying degrees:

- Meeting Regulatory Oversight Responsibilities
- Protecting Systems and Data
- Improving Contract Management
- Ensuring Effective Human Capital Management

Information on the challenge areas and the corresponding audit, evaluation, investigation, or review work are discussed in the attachment. If you have any questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

[1] Pub. L. No. 106-531, § 3a, 114 Stat. 2537-38 (November 22, 2000).

Attachment

cc: Prashant Yerramalli, Chief of Staff, Office of Chair Gensler
Heather Slavkin Corzo, Policy Director, Office of Chair Gensler
Kevin Burris, Counselor to the Chair and Director of Legislative and Intergovernmental Affairs
Scott Schneider, Counselor to the Chair and Director of Public Affairs
Ajay Sutaria, GC Counsel, Office of Chair Gensler
Phillip Havenstein, Operations Counsel, Office of Chair Gensler
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Mark T. Uyeda, Commissioner
Holly Hunter-Ceci, Counsel, Office of Commissioner Uyeda
Jaime Lizárraga, Commissioner
Laura D'Allaird, Counsel, Office of Commissioner Lizárraga
Parisa Haghshenas, Counsel, Office of Commissioner Lizárraga
Dan Berkovitz, General Counsel
Elizabeth McFadden, Deputy General Counsel, General Litigation/Acting Managing Executive
Lisa Helvin, Principal Deputy General Counsel for Adjudication and Oversight
Kenneth Johnson, Chief Operating Officer
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Audit Coordinator/Assistant Chief Risk Officer, Office of Chief Risk Officer

U.S. SECURITIES AND
EXCHANGE COMMISSION

October 13, 2022

OFFICE OF
INSPECTOR
GENERAL

The Inspector General's Statement on the SEC's Management and Performance Challenges

CONTENTS

ABBREVIATIONS

CAT	Consolidated Audit Trail
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
Enforcement	Division of Enforcement
EXAMS	Division of Examinations
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	U.S. Government Accountability Office
IT	information technology
Kearney	Kearney & Company, P.C.
LH	labor-hour
NAICS	North American Industry Classification System
OA	Office of Acquisitions
OASB	Office of the Advocate for Small Business Capital Formation
OHR	Office of Human Resources
OIAD	Office of the Investor Advocate
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OMWI	Office of Minority and Women Inclusion
RIA	registered investment adviser
SAM	System for Award Management
SEC, agency, or Commission	U.S. Securities and Exchange Commission
SLC	Service Level Commitment
T&M	time-and-materials
TCR	tips, complaints, and referrals
TRENDS	Tracking and Reporting Examination National Documentation System
WTTS	Workforce Transformation and Tracking System

CHALLENGE: Meeting Regulatory Oversight Responsibilities

The U.S. Securities and Exchange Commission (SEC, agency, or Commission) is charged with overseeing about $118 trillion in annual securities trading on the United States equity markets and the activities of more than 29,000 registered entities, including investment advisers, mutual funds, exchange-traded funds, broker-dealers, municipal advisors, and transfer agents. The agency also oversees 24 national securities exchanges, 95 alternative trading systems, 10 credit rating agencies, and 7 active registered clearing agencies, as well as the Public Company Accounting Oversight Board, the Financial Industry Regulatory Authority, the Municipal Securities Rulemaking Board, the Securities Investor Protection Corporation, and the Financial Accounting Standards Board. In addition, the SEC is responsible for selectively reviewing the disclosures and financial statements of more than 7,900 reporting companies.

As in previous years, agency management and the Office of Inspector General (OIG) recognize that the SEC's ability to meet its mission of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation becomes more challenging as the markets, products, and participants within the SEC's purview increase in size, number, and complexity. The SEC's strategic plan establishes goals and initiatives to ensure that the agency focuses on the needs of investors, as well as its ability to adapt to rapidly changing markets, new technology, innovation, and evolving global risks.[1]

We describe below the challenges of (1) managing resources while meeting the SEC's regulatory agenda; (2) keeping pace with changing markets and innovations; and (3) leveraging technology and analytics to meet mission requirements and respond to significant developments and trends.

Managing Resources While Meeting the Regulatory Agenda

Rulemaking is the process by which federal agencies implement legislation passed by Congress and signed into law by the President and, as part of its regulatory oversight responsibilities, the SEC creates or updates rules (also referred to as "regulations"). Legislation, such as the Securities Act of 1933,[2] the Securities Exchange Act of 1934,[3] the Investment Company Act of 1940,[4] the Sarbanes-Oxley Act of 2002,[5] and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank)[6] provide the framework for the SEC's oversight of the securities markets. The rulemaking process involves several steps that are designed to give the public an opportunity to provide their opinions on whether the agency should adopt or adopt with modifications a proposed rule. According to the Administrative Procedure Act,[7] agencies must follow an open process when issuing regulations, including publishing a

[1] On October 11, 2018, the SEC issued a strategic plan for fiscal years 2018 to 2022. On August 24, 2022, the SEC released for public comment a draft strategic plan for fiscal years 2022 to 2026. As of the date of this document, the new strategic plan had not been finalized.

[2] Pub. L. 73-22, 48 Stat. 74 (May 27, 1933).

[3] Pub. L. 73-291, 48 Stat. 881 (June 6, 1934).

[4] Pub. L. 76-768, 54 Stat. 789 (August 22, 1940).

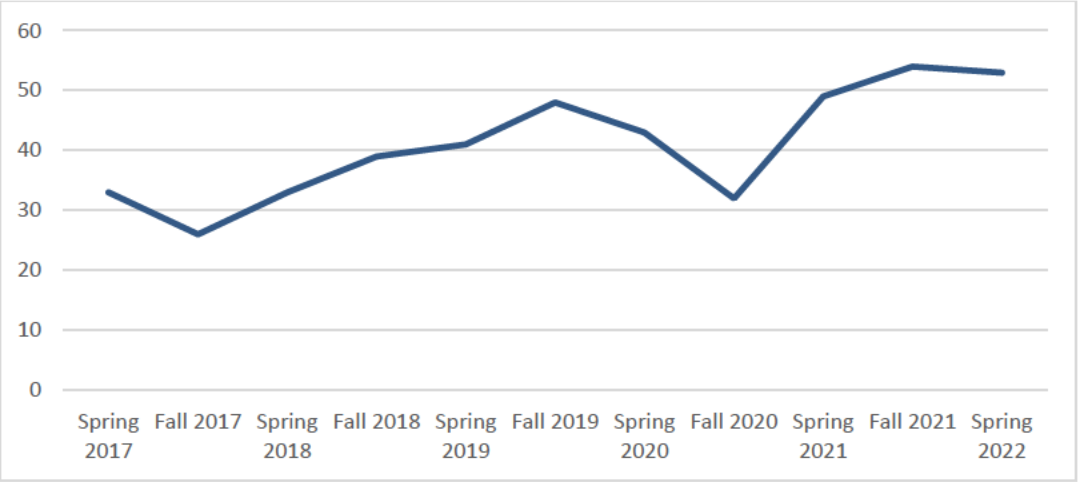
[5] Pub. L. 107-204, 116 Stat. 745 (July 30, 2002).

[6] Pub. L. 111-203, 124 Stat. 1376 (July 21, 2010).

[7] Pub. L. 79-404, 60 Stat. 237, 239 (June 11, 1946).

statement of rulemaking authority in the Federal Register for all proposed and final rules. Moreover, each fall and spring, regulatory agencies are required to publish a regulatory agenda,[8] which is how agencies announce future rulemaking activities and update the public on pending and completed regulatory actions. As Figure 1 shows, the number of rulemaking activities on the SEC's regulatory agenda between spring 2017 and spring 2022 increased overall.

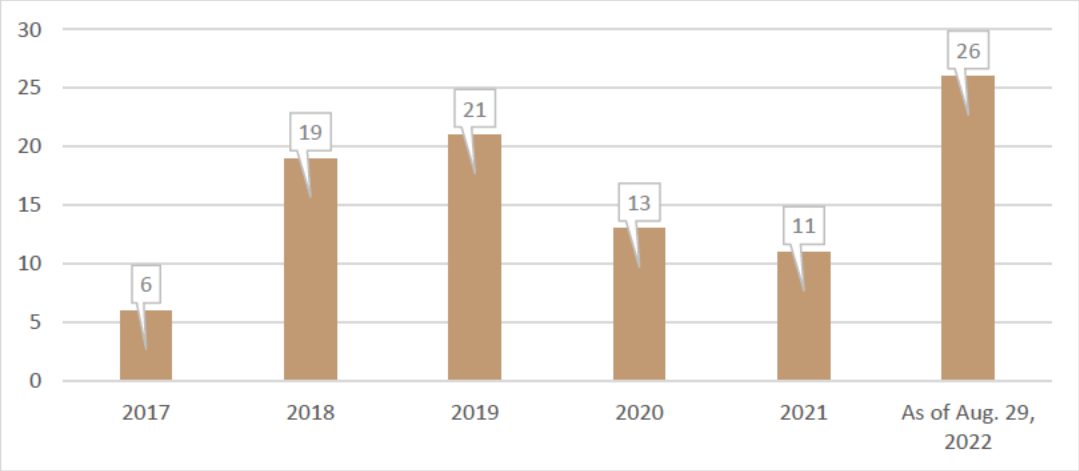
FIGURE 1. Number of Rulemaking Activities on the SEC's Regulatory Agenda (Spring 2017 – Spring 2022)



Source: OIG-generated based on data from the Office of Management and Budget's (OMB) Office of Information and Regulatory Affairs (https://www.reginfo.gov/public/ last accessed on September 8, 2022).

Additionally, in only the first 8 months of 2022, the SEC proposed 26 new rules, which was more than twice as many new rules as proposed the preceding year and more than it had proposed in each of the previous 5 years. (See Figure 2.)

FIGURE 2. Number of New SEC Rules Proposed (2017 – August 2022)



Source: OIG-generated based on data from the SEC (https://www.sec.gov/rules/proposed.shtml, as of August 29, 2022).

[8] Pub. L. 96-354, 94 Stat. 1166 (September 19, 1980).

We met with managers from the SEC's divisions of Trading and Markets, Investment Management, Corporation Finance, and Economic and Risk Analysis, some of whom raised concerns about increased risks and difficulties managing resources and other mission-related work because of the increase in the SEC's rulemaking activities. For example, some reported an overall increase in attrition (discussed further on page 21 of this document) and difficulties hiring individuals with rulemaking experience. In the interim, managers reported relying on detailees, in some cases with little or no experience in rulemaking. Others told us that they may have not received as much feedback during the rulemaking process, either as a result of shortened timelines during the drafting process or because of shortened public comment periods. Although no one we met with identified errors that had been made, some believed that the more aggressive agenda—particularly as it relates to high-profile rules that significantly impact external stakeholders—potentially (1) limits the time available for staff research and analysis, and (2) increases litigation risk. Finally, some managers noted that fewer resources have been available to complete other mission-related work, as rulemaking teams have borrowed staff from other organizational areas to assist with rulemaking activities.

Furthermore, the SEC's rulemaking function relies on coordination and collaboration amongst several agency divisions and offices and, as we reported in our October 2021 statement on the SEC's management and performance challenges, agency leaders should take measures to strengthen communication and coordination across SEC components. Indeed, the SEC's fiscal year (FY) 2021 Agency Financial Report states that the SEC values teamwork and recognizes "that success depends on a skilled, diverse, coordinated team committed to the highest standards of trust, hard work, cooperation, and communication."[9] Additionally, the SEC's strategic plan identifies teamwork of the SEC's staff and its leaders, along with other elements, as the "foundation" of the agency.[10] To support the strategic plan's Goal 3 – "Elevate the SEC's performance by enhancing our analytical capabilities and human capital development" – the SEC committed to the following initiative:

> *3.5 Promote collaboration within and across SEC offices to ensure we are communicating effectively across the agency, including through evaluation of key internal processes that require significant collaboration.*[11]

In response to our October 2021 statement on the SEC's management and performance challenges, agency management re-affirmed its commitment to promoting effective and collaborative information-sharing across the agency.[12] Management's continued attention to strengthening communication and coordination across divisions and offices is instrumental to (1) preventing unintentional negative impacts to divisions and offices when modifying agency-wide processes, (2) maintaining positive trends in employee views on collaboration,[13] and (3) achieving the goals established in the SEC's strategic plan.

[9] U.S. Securities and Exchange Commission, *Fiscal Year 2021 Agency Financial Report*; November 15, 2021.

[10] U.S. Securities and Exchange Commission, *Strategic Plan Fiscal Years 2018-2022*, Goal 3; October 11, 2018.

[11] The agency's draft strategic plan for FY 2022 to FY 2026 (Goal 3) similarly emphasizes the importance of continually strengthening and promoting collaboration within and across SEC offices.

[12] U.S. Securities and Exchange Commission, *Fiscal Year 2021 Agency Financial Report*; November 15, 2021.

[13] With regards to the 2021 Federal Employee Viewpoint survey, 71 percent of agency respondents agreed that SEC managers promote communication among different work units (a 4 percentage point decrease from the previous year). In addition, 75 percent of agency respondents agreed that SEC managers support collaboration across work units to accomplish work objectives (a 3 percentage point decrease from the previous year).

Despite management's commitment to cross-functional collaboration and communication, personnel we met with (including those from the Division of Economic and Risk Analysis, the Division of Enforcement [Enforcement], and the Office of the General Counsel, among others) identified coordination and communication as a persistent challenge in the rulemaking process, particularly given potential overlaps in jurisdiction and differences in opinions. We reported on such challenges in a management letter issued in September 2022.[14] Specifically, we reported that, around December 2021, the Office of the Chair modified the process for coordinating internal reviews of draft agency rules, resulting in the Office of the Advocate for Small Business Capital Formation (OASB)[15] and the Office of the Investor Advocate (OIAD)[16] receiving only fatal flaw drafts of proposed rules[17] for a brief period of time.[18] This change was not formally documented or communicated, and the then-directors of OASB and OIAD were not aware of the change until after it took effect. All parties involved acknowledged that the Office of the Chair has the authority to direct the agency's rulemaking process. Moreover, OASB and OIAD personnel stated that they were generally able to carry out their responsibilities. However, changes to internal processes likely to impact OASB's and OIAD's review and comment related to draft proposed agency rules may unintentionally limit their ability to fulfill their advocacy roles and carry out office functions, and may hinder effective collaboration and information sharing across the agency.[19] Although we did not make any formal recommendations, we encouraged the Office of the Chair to consider, as a management practice, notifying OASB and OIAD before future changes to the rulemaking process, potentially impacting these offices, are implemented.

Keeping Pace With Changing Markets and Innovations

> *Technological advancements and commercial developments continue to change how our securities markets operate and spur the development of new products.*
>
> *Source: U.S. Securities and Exchange Commission, Fiscal Year 2021 Agency Financial Report; November 15, 2021.*

As securities markets continue to grow in size and complexity and technological advancements contribute to changes in how markets operate, the SEC's ability to remain an effective regulator requires that it continuously monitor the market environment, and as appropriate, adjust and modernize its expertise, rules, regulations, and oversight tools and activities. Securities markets have experienced significant growth in recent years, with a record number of families holding direct and indirect stocks, and (as Table 1 shows) a record number of registered investment

[14] U.S. Securities and Exchange Commission, Office of Inspector General, *Final Management Letter: Changes to the Internal Review Process for Proposed Rules May Impact the Office of the Advocate for Small Business Capital Formation and the Office of the Investor Advocate* (September 29, 2022).

[15] The SEC Small Business Advocate Act of 2016 (Pub. L. No. 114-284, 130 Stat. 1447 [December 16, 2016]) requires OASB to advocate for small businesses and their investors by, among other things, analyzing the potential impact on small businesses and small business investors of Commission-proposed regulations that are likely to have a significant economic impact on small businesses and small business capital formation.

[16] Pursuant to Section 915 of Dodd-Frank and codified at Section 4(g) of the Exchange Act of 1934, OIAD is required to analyze the potential impact on investors from proposed rules and regulations of the Commission.

[17] A fatal flaw draft is the last draft circulated before the Commission votes on a proposed rule, often only a few days before the vote. It is typically the final version of the rule, to be reviewed only for critical issues, and will not incorporate policy revisions.

[18] According to agency officials, the change in the rulemaking process was reversed in early 2022.

[19] Other OIG work completed in FY 2022 also highlighted areas where collaboration and communication within the SEC could be improved. *See* U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Can Improve in Several Areas Related to Hiring* (Report No. 572; February 28, 2022).

TABLE 1. Number of RIAs (FY 2018 – July 2022)

Date	Number of RIAs
Beginning of FY 2018	12,616
Beginning of FY 2019	13,222
Beginning of FY 2020	13,458
Beginning of FY 2021	13,810
Beginning of FY 2022	14,719
As of July 1, 2022	15,167

Source: OIG-generated based on data provided by EXAMS.

advisers (RIA), which represent the largest portion of the registered firm population overseen by the SEC's Division of Examinations (EXAMS).

In addition, as noted in a March 2022 White House fact sheet accompanying a new Executive Order, the crypto market is highly concentrated and has seen explosive growth in recent years, surpassing a $3 trillion market cap last November, up from $14 billion just 5 years ago.[20] The new Executive Order outlines a national policy for digital assets to include protecting consumers, investors, and businesses.[21]

In recognition of the need to protect investors and respond to the changing environment, the SEC is taking steps to address the increasing risks related to the crypto market such as (1) getting platforms registered and regulated much like exchanges; (2) coordinating with the Commodity Futures Trading Commission on determining how best to regulate platforms where trading of securities and non-securities is intertwined; and (3) identifying how to work with platforms and best ensure the protection of customers' assets. Additionally, the SEC recently announced the allocation of 20 additional positions for Enforcement's Crypto Assets and Cyber Unit, nearly doubling its size, as the volatile and speculative crypto marketplace has attracted tens of millions of American investors and traders.[22] As the SEC continues to increase its workforce and take other steps to protect investors, there is uncertainty about which agency—the SEC or the Commodity Futures Trading Commission—will have regulatory oversight responsibilities over the crypto market and what legal tools and authorities will be available. Such uncertainty can unsettle market factors and elevate risk for Main Street investors.

EXAMS also recognizes and strives to adapt to changing market factors. In its 2022 Examinations Priorities,[23] EXAMS noted significant focus areas that pose unique or emerging risks to investors or the markets, such as environmental, social, and governance investing; standards of conduct issues for broker-dealers and RIAs; and emerging technologies and crypto-assets, among others. EXAMS will continue to conduct examinations of broker-dealers and RIAs, many of which use developing financial technologies, and market participants engaged with crypto-assets, with a continued need to optimize its limited resources as it works to improve and promote compliance with regulatory requirements.

In a report we issued in January 2022, we noted steps EXAMS took to optimize its limited resources and increase efficiency and effectiveness, to include the following:

[20] The White House (March 9, 2022). *FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets*.

[21] *Executive Order on Ensuring Responsible Development of Digital Assets*; March 9, 2022.

[22] Gurbir S. Grewal Director, Division of Enforcement, Testimony on "Oversight of the SEC's Division of Enforcement" Before the United States House of Representatives Committee on Financial Services Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets; July 21, 2022.

[23] U.S. Securities and Exchange Commission, *Division of Examinations 2022 Examination Priorities;* March 30, 2022.

- Moved its Tracking and Reporting Examination National Documentation System (TRENDS) to a new, cloud-based platform, which is expected to improve the system's adaptability, workflow capability, and data standardization;
- Launched a new examination support service, which among other things, assists examiners with data staging, cleansing, transformation, enrichment, and analysis; and
- Advanced its centralized asset verification program, which, according to EXAMS management, has enabled growth in the number of exams involving asset verification, as well as the amount of assets verified during these exams.[24]

Although EXAMS took these and other steps to increase efficiencies, we also reported that controls over the RIA examination planning processes needed improvement. Specifically, we found some staff commenced substantive RIA examination procedures before management approved the examination pre-fieldwork phase, and staff did not always consistently maintain key documents in TRENDS. In addition, we were unable to find documentation indicating that an examination supervisor notified registrants of non-EXAMS staff participation, as required.

We recommended that management (1) develop controls that help ensure timely supervisory approval of an examination's pre-fieldwork phase; (2) reiterate to examination staff and management the importance of and requirements for timely supervisory approval of each examination's pre-fieldwork phase; and (3) review examination documentation requirements regarding communications with registrants to ensure they are clear and examiners maintain such documentation in a consistent manner, and update examination policies as needed. Management concurred with our recommendations, which, as of the date of this document, are open and will be closed upon completion and verification of corrective action taken.

As we begin FY 2023, we will continue to monitor agency plans and actions to improve controls around supervisory approval of examinations' pre-fieldwork phase and documentation requirements regarding communications with registrants.

Use of Technology and Analytics to Meet Mission Requirements and Respond to Significant Developments and Trends

As we reported in previous years, agency management and the OIG continue to recognize the importance of technology and analytics in the SEC's ability to efficiently and effectively meet mission requirements and respond to significant developments and trends in the evolving capital markets. The SEC's strategic plan (Goals 2 and 3, and related strategic initiatives) reflects the importance of these efforts.[25] Additionally, according to the SEC's FY 2023 Congressional Budget Justification, the economy's reliance on the rapidly changing field of data analytics is growing, and the Commission needs to adjust by

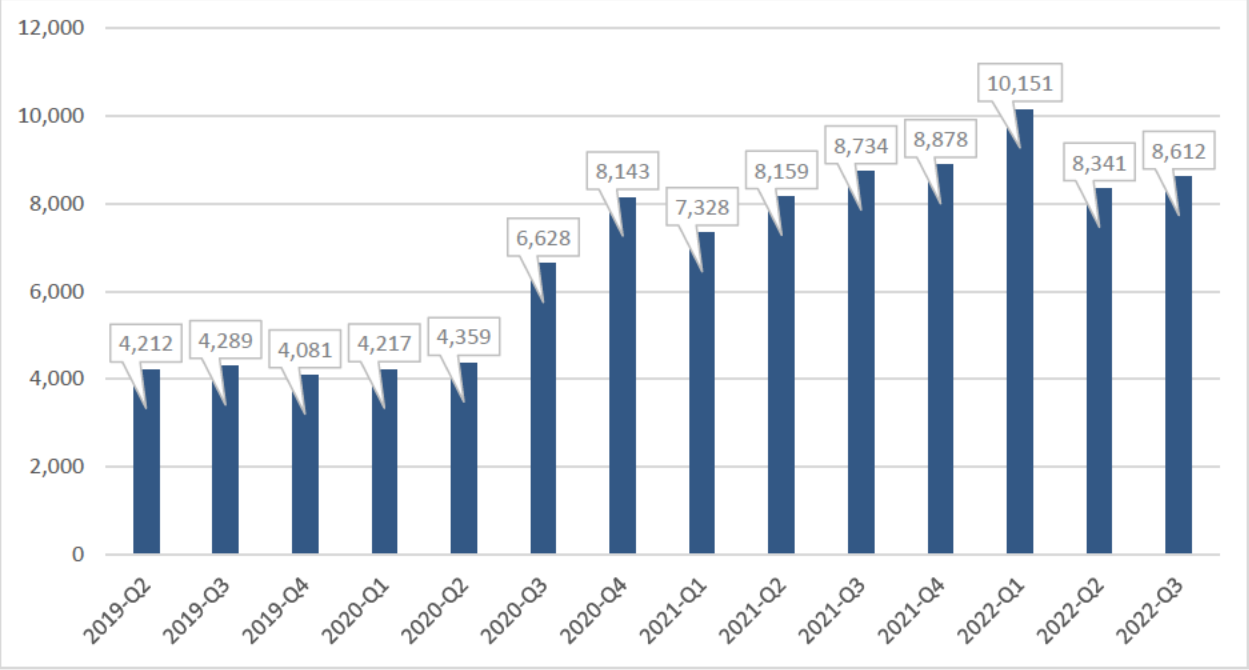
[24] U.S. Securities and Exchange Commission, Office of Inspector General, *Registered Investment Adviser Examinations: EXAMS Has Made Progress To Assess Risk and Optimize Limited Resources, But Could Further Improve Controls Over Some Processes* (Report No. 571, January 25, 2022).

[25] The agency's draft strategic plan for FY 2022 to FY 2026 (Goals 1, 2, and 3) similarly emphasizes that the SEC must effectively use technology and data.

re-evaluating how it assesses data and incorporates machine learning and deep learning into its examination and enforcement functions.[26]

Notably, Enforcement analyzes a massive volume of data each year including thousands of tips, complaints, and referrals (TCR) related to allegations of possible violations of the federal securities laws or conduct that poses a risk of harm to investors. Enforcement receives TCRs from the public, self-regulatory organizations, other federal and local agencies, and other entities. As Figure 3 shows, the SEC received a record number of TCRs in the first quarter of 2022.

FIGURE 3. Number of TCRs Received (2019, Quarter 2 – 2022, Quarter 3)



Source: OIG-generated based on data provided by Enforcement's Office of Market Intelligence. FY 2021 totals exclude 12,935 TCRs related to the market volatility event, and totals exclude TCRs submitted as test TCRs to validate the system.

In an evaluation report we issued in February 2021, we reported on the SEC's process to plan and develop a future TCR system and we recommended actions to further strengthen the SEC's TCR program and TCR system management and development.[27] We also encouraged management to monitor the upward trend in TCRs, and determine whether additional actions, resources, or staff allocations were needed. Management has since taken actions to address our recommendations and is working to implement a new TCR management system. According to Enforcement's Office of Market Intelligence, the organization implemented a risk-based process to assess and triage TCRs through the use of analytics and automation, which will be incorporated into the new TCR system. In planning for the new system, the agency continues to assess the application and data, conduct market research on potential technologies, and prepare a strategic plan.

[26] U.S. Securities and Exchange Commission, *Fiscal Year 2023 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2021 Annual Performance Report*; March 28, 2022.

[27] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Can Further Strengthen the Tips, Complaints, and Referrals Program* (Report No. 566; February 24, 2021).

Although we acknowledge the Office of Market Intelligence's use of analytics and implementation of a new TCR system, the TCR program—along with many other critical programs and systems within the SEC—must rely on personnel to correctly input data into systems. For example, with the handling of TCRs, agency staff from divisions and offices must be sure to correctly transfer TCRs to the Office of Market Intelligence. As noted in a management letter our office issued in May 2021, we identified 2 matters of 3,303 we reviewed that were not transferred from the Office of Investor Education and Advocacy to the TCR system.[28] Moreover, in FY 2022, we investigated the former SEC Ombudsman and found that the former Ombudsman failed to enter TCRs on investor matters received by the Office of the Ombudsman that warranted entry, as required by the SEC's *Commission-Wide Policies and Procedures for Handling TCRs*. Specifically, the agency's policy and corresponding administrative regulation[29] state that all SEC staff are responsible for entering TCRs into the TCR system or forwarding them to a TCR point of contact within specified timeframes, and "when in doubt, staff should err on the side of entering a TCR." Instead, the former Ombudsman directed staff within the Office of the Ombudsman to refer investors to enter their own TCRs on matters related to alleged securities law violations or fraud. As previously noted, through the TCR program, the SEC receives and responds to credible allegations of possible violations of the federal securities laws. Improper handling of TCRs may impede the SEC's ability to timely and effectively protect investors.

Improper handling of TCRs may impede SEC investor protection efforts

Ongoing and Anticipated OIG Work. In FY 2023, we will continue to assess how well the SEC effectively and efficiently meets its regulatory oversight responsibilities. We will follow-up on open recommendations intended to improve controls around the examination program, and we will complete an ongoing audit of the SEC's whistleblower program and an evaluation of Enforcement's efforts and goals to expedite investigations, where possible and appropriate. Finally, we will initiate a review of the SEC's oversight of entity compliance with Regulation Best Interest and Form CRS.[30]

[28] U.S. Securities and Exchange Commission, Office of Inspector General, *Final Management Letter: Actions May Be Needed To Improve Processes for Receiving and Coordinating Investor Submissions* (May 24, 2021).

[29] U.S. Securities and Exchange Commission, SEC Administrative Regulation 3-2, *Tips, Complaints, and Referrals (TCR) Intake Policy*; November 29, 2016.

[30] Regulation Best Interest, the new Form CRS Relationship Summary, and two separate interpretations under the Investment Advisers Act of 1940 are part of a package of rulemakings and interpretations adopted by the Commission on June 5, 2019, to enhance and clarify the standards of conduct applicable to broker-dealers and investment advisers, help retail investors better understand and compare the services offered and make an informed choice of the relationship best suited to their needs and circumstances, and foster greater consistency in the level of protections provided by each regime, particularly at the point in time that a recommendation is made.

CHALLENGE: Protecting Systems and Data

Because the work of the SEC touches nearly every part of the nation's capital markets and advances international regulatory, supervisory, and enforcement cooperation, it is critically important to protect agency systems and data. In 2022, the Administration along with the Cybersecurity and Infrastructure Security Agency (CISA) warned that malicious cyber activity against the United States homeland could have an impact on our nation's organizations, and threats are more pronounced because of international events.[31] The U.S. Government Accountability Office (GAO) also reported that cyber risks are growing, and cyberattacks targeting critical infrastructure—including financial services—could affect entire systems and result in catastrophic financial loss.[32] Individuals or groups with malicious intentions attempt to intrude into agency systems to obtain sensitive information, commit fraud and identity theft, disrupt agency operations, or launch attacks against other systems and networks. Even in the absence of those intentions, inadequate safeguards can lead to the unauthorized disclosure, modification, use, or disruption of information that can compromise the integrity of agency operations. Therefore, the SEC must continue to take steps to safeguard the security, integrity, and availability of its information systems and sensitive data.

SEC management has recognized that "efficient, effective, and responsible use of data and information technology (IT) is a crucial focus of the agency."[33] In its FY 2023 Congressional Budget Justification, the agency requested additional funds for IT initiatives to expand progress in key areas such as cybersecurity, secure cloud infrastructure, and data management. CISA is also continuing to publish guidance to make the federal civilian workforce more resilient to cyber threats.

> *A critical element of the SEC's strategy is to protect the agency's two most important assets, its people and its data, both of which are vital to executing the SEC's mission.*
>
> *Source: U.S. Securities and Exchange Commission, Fiscal Year 2021 Agency Financial Report; November 15, 2021.*

The SEC's FY 2023 budget request addresses plans to hire additional personnel within the Office of Information Technology (OIT) who would provide expertise in cloud computing; strengthen security controls, policies, and procedures; and help the agency comply with requirements mandated in a recent Executive Order to move the agency toward a "zero trust" approach to cybersecurity.[34] Additionally, as we describe further below, opportunities exist to better protect SEC systems and data, including by evaluating and addressing the underlying cause(s) and impact of a material weakness related to insufficient user access controls, strengthening the agency's cybersecurity posture, and continuing to mature its information security program.

---

[31] The White House (March 21, 2022). *FACT SHEET: Act Now to Protect Against Potential Cyberattacks;* and CISA, *Shields Up* website (https://www.cisa.gov/shields-up, last accessed on September 9, 2022).

[32] U.S. Government Accountability Office, *CYBER INSURANCE Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (GAO-22-104256, June 2022).

[33] U.S. Securities and Exchange Commission, *Fiscal Year 2023 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2021 Annual Performance Report;* March 28, 2022.

[34] Executive Order 10460, *Improving the Nation's Cybersecurity*; May 12, 2021.

Evaluating and Addressing the Cause(s) and Impact of a Material Weakness Related to Insufficient User Access Controls

In its FY 2021 Agency Financial Report, the SEC disclosed a newly discovered material weakness associated with lack of controls related to user access to a Commission system. Specifically, the SEC reported that the information tracking and document storage system for documents related to recommendations for certain Commission actions did not include controls sufficient to prevent access by staff who should not view such documents.[35] This is important because, while the Commission has both investigatory and adjudicatory responsibilities, the Administrative Procedure Act contemplates the separation of those functions among the agency staff who assist the Commission in each.[36] Therefore, agency employees who are investigating or prosecuting an adjudicatory matter before the Commission generally may not participate in the Commission's decision-making in that or a factually related matter. However, the identified user access control deficiency did not ensure the necessary separation of the Commission's enforcement and adjudicatory functions for administrative adjudications. The SEC's FY 2021 Agency Financial Report further noted that, while a review of the affected system was underway, action had been taken to remediate the control deficiency.

Then, in April 2022, the Commission released a statement that provided additional information about the control deficiency, along with the results of the SEC's review of the impact of the control deficiency on two ongoing federal court litigations: *SEC v. Cochran*, No. 21-1239 (S. Ct.), and *Jarkesy v. SEC*, No. 20-61007 (5th Cir.). The statement reads, in part:

> *The Commission has determined that, for a period of time, certain databases maintained by the Commission's Office of the Secretary were not configured to restrict access by Enforcement personnel to memoranda drafted by Adjudication staff. As a result, in a number of adjudicatory matters, administrative support personnel from Enforcement, who were responsible for maintaining Enforcement's case files, accessed Adjudication memoranda via the Office of the Secretary's databases. Those individuals then emailed Adjudication memoranda to other administrative staff who in many cases uploaded the files into Enforcement databases.*[37]

With respect to these two matters, according to the Commission's statement, agency enforcement staff had access to certain adjudicatory memoranda, but this access "did not impact the actions taken by the staff investigating and prosecuting the cases or the Commission's decision-making in the matters."

The SEC is continuing to review and has not yet disclosed the full impact the internal control deficiency caused by the insufficient user access controls had on the remaining affected adjudicatory matters. The Commission's statement indicated that the agency's review team will continue to assess the remaining

[35] U.S. Securities and Exchange Commission, *Agency Financial Report Fiscal Year 2021*; November 15, 2021.

[36] Pub. L. 79-404 60 Stat. 240 (June 11, 1946).

[37] U.S. Securities and Exchange Commission, *Commission Statement Relating to Certain Administrative Adjudications*; April 5, 2022.

affected adjudicatory matters, and additional findings will be published "in the near future." Furthermore, the Commission stated that, going forward, it will work to better protect the separation of adjudicatory work-product within the system for administrative adjudications, including by enhancing systems for controlling access to Adjudication memoranda.

In conjunction with the ongoing FY 2022 evaluation of the SEC's implementation of the Federal Information Security Modernization Act of 2014 (FISMA), we assessed the SEC's incident response related to this control deficiency, and found that the agency generally complied with applicable requirements. Nonetheless, the OIG will continue to independently review the control deficiency to understand and, as appropriate, report the full impact of this material weakness. We also will continue to monitor the agency's progress towards redesigning or replacing the systems in question.

Strengthening the SEC's Cybersecurity Posture

The SEC is aware that protecting information systems and data is a priority, as cyber actors may exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a system. In FY 2022, the SEC's OIT made progress by taking corrective action sufficient to close one cybersecurity-related recommendation from a previous OIG report.[38] However, as Table 2 summarizes, work remains to close other cybersecurity-related recommendations we issued before FY 2021.

TABLE 2. Certain Open Cybersecurity Recommendations as of October 2022*

Report Title	Date Issued	Recommendation(s)
Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services (Report No. 562)	9/30/20	Recommendations 5 and 6 Current estimated corrective action completion date: February 2023

Source: OIG-generated based on recommendation tracking and follow-up records.

** This does not include recommendations issued in connection with mandated annual information security evaluations, which we discuss on pages 13 and 14 of this document.*

Recognizing there is more work to be done, in FY 2023, the SEC plans to increase efforts to:

- Support the implementation of security services within agency-selected cloud capabilities.
- Enhance identity, access, and privilege management protocols and operations across platforms.
- Modernize security operations capabilities focusing on automation, integration of shared services and experts through managed services, and proactive capabilities to identify threats.
- Continue the implementation of a secure application development structure across all agency development teams and projects.[39]

[38] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (Report No. 556; Nov. 7, 2019), Recommendation 3.

[39] U.S. Securities and Exchange Commission, *Fiscal Year 2023 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2021 Annual Performance Report;* March 28, 2022.

The SEC also has an open recommendation from a recent GAO report on assessing security controls related to telework. The CARES Act of 2020 contains a provision for GAO to monitor the federal response to the pandemic. Specifically, GAO was asked to examine federal agencies' preparedness to support expanded telework. In September 2021, GAO issued its report, which contained two recommendations for the SEC regarding the assessment and documentation of relevant IT security controls and enhancements.[40] Although the agency's comments to the report state that the SEC expected to complete actions to remediate the recommendations by the second quarter of FY 2022, as of September 15, 2022, remediation work was still underway for the recommendation related to ensuring that the agency documents relevant IT security controls and enhancements in the security plan for the system that provides remote access for telework. GAO concluded that if agencies do not sufficiently document relevant security controls, assess the controls, and fully document remedial actions for weaknesses identified in security controls, then agencies are at increased risk that vulnerabilities in their systems that provide remote access could be exploited.

The SEC also faces cybersecurity challenges with respect to its access, use, and security of data available through the Consolidated Audit Trail (CAT). Pursuant to an SEC rule (Rule 613), self-regulatory organizations have submitted a national market system plan to create, implement, and maintain a consolidated order tracking system, or CAT, that when fully implemented will capture customer and order event information for orders in national market system securities, across all markets, from the time of order inception through routing, cancellation, modification, or execution. In its FY 2023 budget request, the SEC noted that the CAT continues to roll out functionality as the phased launch of broker-dealer reporting and regulator functionality progresses. Because CAT data is highly sensitive, the SEC must continue working to establish an environment and applications to appropriately secure the data accessed and used by the SEC as it becomes available.

Maturing the SEC's Information Security Program

Effective information security controls are essential to protecting the SEC's information systems and the data contained therein. To help the SEC establish and maintain effective information security controls and to comply with FISMA, the OIG annually evaluates the SEC's implementation of FISMA information security requirements and the effectiveness of the agency's information security program on a maturity model scale.[41] The OIG contracted with Kearney & Company, P.C. (Kearney) to conduct the FY 2021 independent evaluation and, on December 21, 2021, issued the report titled, *Fiscal Year 2021 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 570).[42]

As stated in Report No. 570, since FY 2020, OIT improved aspects of the SEC's information security program. Among other actions taken, the SEC refined its management of security training roles and responsibilities, enhanced its security training strategy, implemented the agency's policy for specialized security training, optimized a vulnerability disclosure policy, refined its configuration management

[40] U.S. Government Accountability Office, *COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls* (GAO-21-583, September 2021).

[41] Pub. L. No. 113-283, § 3555, 128 Stat. 3073 (2014).

[42] As previously stated, the FY 2022 FISMA evaluation is ongoing and will be completed in the first quarter of FY 2023.

processes related to reconciliation of software code in production, improved its incident response information-sharing capabilities, and improved its contingency planning capabilities. Notably, these improvements occurred despite the unique challenges presented by Coronavirus Disease 2019 (COVID-19).

In FY 2021, the SEC's maturity level was primarily "Consistently Implemented" or "Managed and Measurable"

Although the SEC strengthened its program, Kearney determined for FY 2021 that the agency's information security program did not meet annual Inspector General FISMA reporting metrics' definition of "effective," which requires the simple majority of domains to be rated as Level 4 ("Managed and Measurable").[43] As stated in Report No. 570, the SEC's maturity level for the five Cybersecurity Framework security functions ("identify," "protect," "detect," "respond," and "recover") and related domains was primarily Level 3 ("Consistently Implemented") or Level 4 ("Managed and Measurable"). Although the SEC's program, as a whole, did not reach the level of an effective information security program, the agency showed significant improvement at the domain level. Specifically, the agency's assessed maturity level for the Security Training domain increased from Level 2 ("Defined") to Level 5 ("Optimized"). Table 3 shows the SEC's FISMA ratings in FY 2020 and FY 2021.

TABLE 3. Summary of SEC FISMA Ratings (FY 2020 and FY 2021)

Domain	Assessed Rating By FY	
	2021	2020
Risk Management	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Supply Chain Risk Management	Level 1: *Ad Hoc*	*Not Applicable*
Configuration Management	Level 2: *Defined*	Level 2: *Defined*
Identity and Access Management	Level 2: *Defined*	Level 2: *Defined*
Data Protection and Privacy	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Security Training	Level 5: *Optimized*	Level 2: *Defined*
Information Security Continuous Monitoring	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Incident Response	Level 4: *Managed and Measurable*	Level 4: *Managed and Measurable*
Contingency Planning	Level 4: *Managed and Measurable*	Level 4: *Managed and Measurable*

Source: OIG-generated based on Exhibit 1 from Report No. 570.

Report No. 570 included eight new recommendations to strengthen the SEC's information security program, and highlighted opportunities to improve in all nine FY 2021 Inspector General FISMA reporting metric areas. To date, the SEC has taken corrective action sufficient to close three of these eight recommendations. However, five recommendations from prior year FISMA reports remain open (two from

[43] *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1*; May 12, 2021.

FY 2017,[44] one from FY 2018,[45] and two from FY 2020[46]). We commend agency management for the actions taken to date, and encourage management to promptly act on all opportunities for improvement identified in previous FISMA reports to help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information, and to assist the agency's information security program reach the next maturity level.

Finally, we continue to track the agency's progress related to an audit of the SEC's enterprise architecture (*Additional Steps Are Needed For the SEC To Implement a Well-Defined Enterprise Architecture*; Report No. 568, issued September 29, 2021). In our report, we highlighted six recommendations to improve the SEC's implementation of a well-defined enterprise architecture (four of which remain open), and one recommendation to improve the SEC's oversight of enterprise architecture support services contracts (which is closed). We understand that the agency has efforts underway to develop an enterprise roadmap for future years, and the remaining four recommendations will be closed upon completion and verification of corrective action taken.

Fully implementing recommended corrective actions from these audits and evaluations may assist the SEC as it seeks to mature aspects of its information security program, generally, and its IT program and program management, specifically.

Ongoing and Anticipated OIG Work. In FY 2023, we will continue to assess the SEC's efforts to secure its systems and data and mature its information security program. Specifically, we will continue to assess the reported user access control deficiency matter, follow-up on open recommendations, complete the ongoing FY 2022 FISMA evaluation, and initiate the FY 2023 FISMA evaluation. We will also review the SEC's efforts to establish a secure environment and applications to use CAT data, determine whether the SEC implemented adequate security controls to safeguard information and IT resources during maximum telework, and assess steps the SEC has planned or taken to address "zero trust" requirements.

[44] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546; March 30, 2018).

[45] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552; December 17, 2018).

[46] U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 563; December 21, 2020).

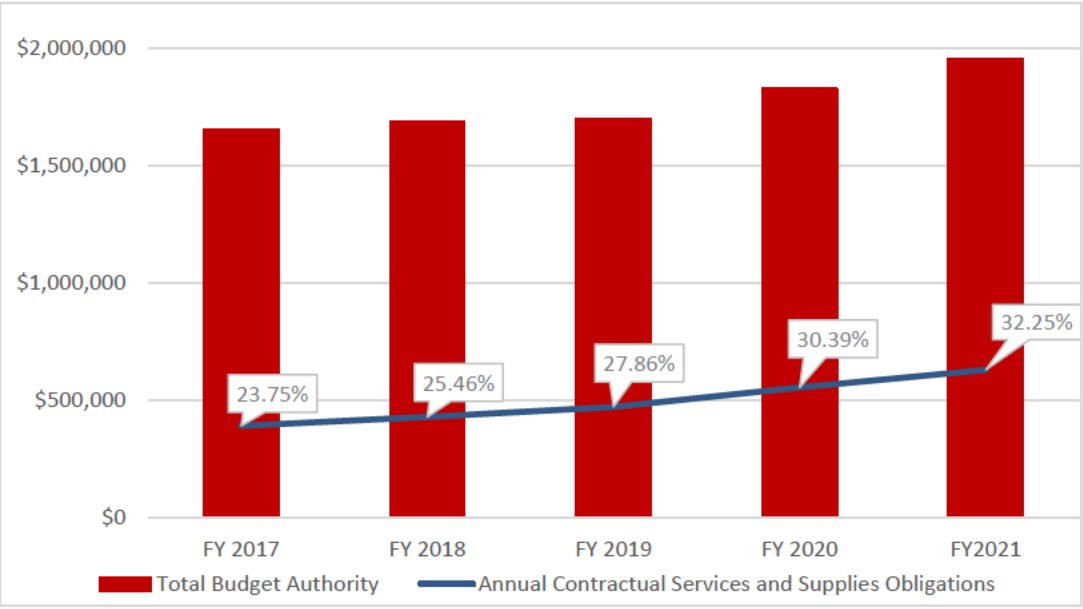
CHALLENGE: Improving Contract Management

Synopsis and Trends in SEC Contracting

The SEC substantially relies on contractor support to accomplish its mission. Contractor support is obtained through a variety of methods, including enterprise-wide contracts, U.S. General Services Administration multiple award schedule contracts, government-wide acquisition contracts, and multi-agency contracts. As markets are ever evolving and increasing in complexity, the SEC relies on contractors for technical and subject matter expertise including, but not limited to, professional legal and investigation-related services; support in areas of accounting, analytics, and examinations; and human resources support services.

To fund its contract requirements, the SEC's FY 2023 budget request included nearly $610 million for contractual services and supplies,[47] which represents about 28 percent of the total $2.149 billion requested for agency operations. As we reported in last year's statement on the SEC's management and performance challenges, annual obligations for contractual services and supplies, when expressed as a percentage of the SEC's total annual budget authority, has been increasing. This trend continued in FY 2021, with annual obligations for contractual services and supplies equaling about 32 percent of the SEC's total annual budget authority. (See Figure 4.)

FIGURE 4. SEC Annual Contractual Services and Supplies Obligations, in Thousands, as a Percentage of Total Annual Budgetary Authority (FY 2017 – FY 2021)

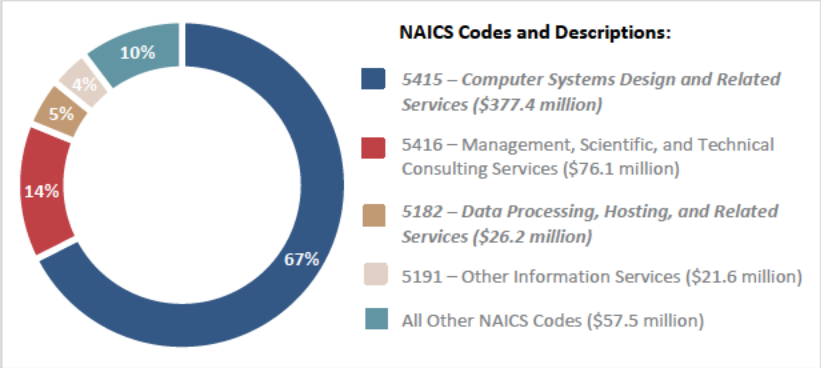


Source: OIG-generated based on annual actual obligations by object class as reported in the SEC's Congressional Budget Justifications for FY 2019 through FY 2023.

[47] According to OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (August 2022), the contractual services and supplies object class covers purchases in object classes 21.0 through 26.0 (Travel and transportation of persons; Transportation of things; Rent, Communications, and Utilities; Printing and reproduction; Other contractual services; and Supplies and materials).

As contract obligations are approaching nearly a third of the agency's annual budget authority, it is essential that the SEC's acquisition workforce effectively manage these resources. Government contracts continue to be an attractive target for fraudsters. In 2021, GAO issued two reports related to contract fraud schemes within the government, focusing on programs within the Department of Defense and the Department of Energy.[48] The SEC is not invulnerable to such schemes and must remain vigilant, closely monitoring areas of risk. For example, GAO identified fraudulent billing schemes as a risk to the procurement process, and the SEC OIG has participated in cross-agency investigative efforts to fight fraudsters who impersonate government officials and submit false purchase orders associated with real government contracts, the terms of which are publicly available.

FIGURE 5. Top NAICS Codes Associated With the SEC's FY 2022 Contract Obligations



Source: OIG-generated from data retrieved from SAM.gov on October 6, 2022.

Although the SEC procures a wide range of services and supplies, the majority of the agency's contract support by dollars obligated is for IT services. These services include, among others, application management, business solutions delivery, IT infrastructure and support services, information security, IT governance and program strategy, data management, and software services. We reviewed the top North American Industry Classification System (NAICS) codes[49] associated with SEC contracts in FY 2022, as reported through the System for Award Management (*SAM.gov*),[50] and noted that, of the nearly $560 million obligated to contract actions that year and included in the system, the SEC obligated about 72 percent (or about $404 million) to vendors doing business under just two IT service-related NAICS codes: one for computer systems design and related services, and another for data processing, hosting, and related services. (See Figure 5.) This represents a slight increase over FY 2021 and a more significant increase over FY 2020 (when obligations under the same two NAICS codes totaled about $401 million and $351 million, respectively).[51]

[48] U.S. Government Accountability Office, *DOD FRAUD RISK MANAGEMENT Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks* (GAO-21-309, August 2021); and *DEPARTMENT OF ENERGY CONTRACTING Improvements Needed to Ensure DOE Assesses Its Full Range of Contracting Fraud Risks* (GAO-21-44, January 2021).

[49] NAICS is a comprehensive industry classification system that covers all economic activities and groups establishments into industries based on the similarity of their production processes. Among other things, U.S. statistical agencies use NAICS to provide uniformity and comparability in the presentation of statistical data describing the U.S. economy. Federal Acquisition Regulation 19.102(b) requires contracting officers to assign one NAICS code to all government solicitations, contracts, and task and delivery orders based on the product or service being acquired and its principal purpose. In this document, "top NAICS codes" refers to those codes that represent the largest amounts in terms of total annual amounts obligated.

[50] SAM is a U.S. General Services Administration Federal Government computer system that, among other things, allows users to create and run reports of detailed information on contract actions that are required to be reported by federal agencies. These are actions with an estimated value of $10,000 or more.

[51] Based on data retrieved from *SAM.gov* on October 6, 2022.

A growing majority of contract support concentrated in IT services—and, therefore, in those segments of the agency's acquisition workforce that procure, administer, and oversee contracts for such services—potentially increases the risk to the SEC. Indeed, since 2015, GAO has reported that management of IT acquisitions and operations is a high risk area needing attention by the executive branch and Congress, stating, "federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. These investments often suffer from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance."[52] We have previously reported on needed improvements in the SEC's management of IT investments.[53] And while last July the SEC completed efforts sufficient to close our remaining recommendations for corrective action stemming from that report, the agency has also increased its investments (and, therefore, its potential risk) related to IT service contracts.

Management of IT acquisitions and operations is a high risk area across the executive branch

Notably, the SEC procures many of its IT services through its OneIT enterprise contract vehicle, which has a 10-year ordering period and a contract ceiling of $2.5 billion. In September 2018, the SEC began awarding time-and-material (T&M), labor-hour (LH), and firm-fixed price task orders under the OneIT contract vehicle, which included separate pools for small businesses only (restricted) and all awardees, including large businesses (unrestricted). As of June 2022, the agency had awarded task orders to 27 companies, including 5 large businesses and 22 small businesses, obligating a total of almost $450 million for task orders under this vehicle. The SEC's Office of Minority and Women Inclusion (OMWI) collaborated with key stakeholders to advertise to vendors opportunities and specifics of the OneIT program. This advertising included a publically available brochure targeted to minority-owned and women-owned businesses. OMWI received positive feedback and is looking to expand the concept to other large SEC contracts being awarded. As such, the SEC's Office of Acquisitions (OA) and OMWI are continuing to work collaboratively to increase outreach to minority-owned and women-owned businesses and continue efforts to increase the SEC's vendor diversity.

Focus on Diversity, Equity, and Inclusion

OA and OMWI are collaborating to voluntarily implement the requirements of Executive Order 13895, which states that the federal government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality.[54] This advancing of equality includes promoting equitable delivery of government benefits and equitable opportunities, such as government contracting and procurement opportunities, which should be available on an equal basis to all eligible providers of goods and services.

[52] U.S. Government Accountability Office, *HIGH-RISK SERIES Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP, March 2021).

[53] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed* (Report No. 555; September 19, 2019).

[54] Executive Order 13895, *Advancing Racial Equity and Support for Underserved Communities through the Federal Government*; January 20, 2021. Independent agencies are strongly encouraged to comply with the provisions of this Executive Order.

Additionally, recent OMB guidance implements commitments to increase the share of contracts awarded to small disadvantaged businesses to 15 percent by 2025.[55] To do this, OMB directs federal agencies to take specific management actions, including increasing the number of new entrants to the federal marketplace and reversing the general decline in the small business supplier base.

Diversity, equity, and inclusion is a focus of OA and, in its FY 2023 budget request, OA requested two additional positions to support a number of priorities, including support for workload increases to review and expand diversity, equity, and inclusion efforts in contracting opportunities. Furthermore, OMWI continues to collaborate with OA to promote access to contracting and sub-contracting opportunities for minority-owned and women-owned businesses, through outreach activities. In March 2022, we initiated an audit to (1) assess the SEC's processes for encouraging small business participation in agency contracting, in accordance with federal laws and regulations; and (2) determine whether, in FYs 2020 and 2021, the SEC accurately reported small business awards. The audit is ongoing and will be completed in FY 2023.

T&M Contracts

Since our 2019 statement on the SEC's management and performance challenges, we have reported that T&M contracts (including LH contracts) lack incentives for contractors to control costs or use labor efficiently and, therefore, are considered higher-risk.[56] Last year, we noted again that the SEC's use of T&M contracts has continued to increase. We encouraged management to assess the SEC's use of these contracts and to formulate actions to reduce their use whenever possible. In response, agency management committed to continuing to closely monitor its use of T&M contracts and "exercise rigorous oversight of these types of contracts."[57] Management further noted that OA has made a number of improvements to better manage T&M contracts, including a new independent government cost estimate guide, contract compliance reviews, information sharing on T&M invoicing, and an automated determination and findings workflow for "more robust and consistent support for the use of T&M" contracts. To date, we have not fully assessed the effectiveness of management's reported additional controls;[58] however, the annual amount obligated to T&M contracts continues to raise concerns about risk to the SEC. As Figure 6 shows, according to data from *usaspending.gov*, the total amount obligated to T&M contracts increased since FY 2018 from about 40 percent to about 53 percent of all SEC contract obligations (which are declining).[59] In addition, as of October 7, 2022, 476 of the SEC's 1,055 total active contracts (or about 45 percent) were T&M contracts.

[55] Office of Management and Budget, Memorandum M-22-03, *Advancing Equity in Federal Procurement*; December 2, 2021.

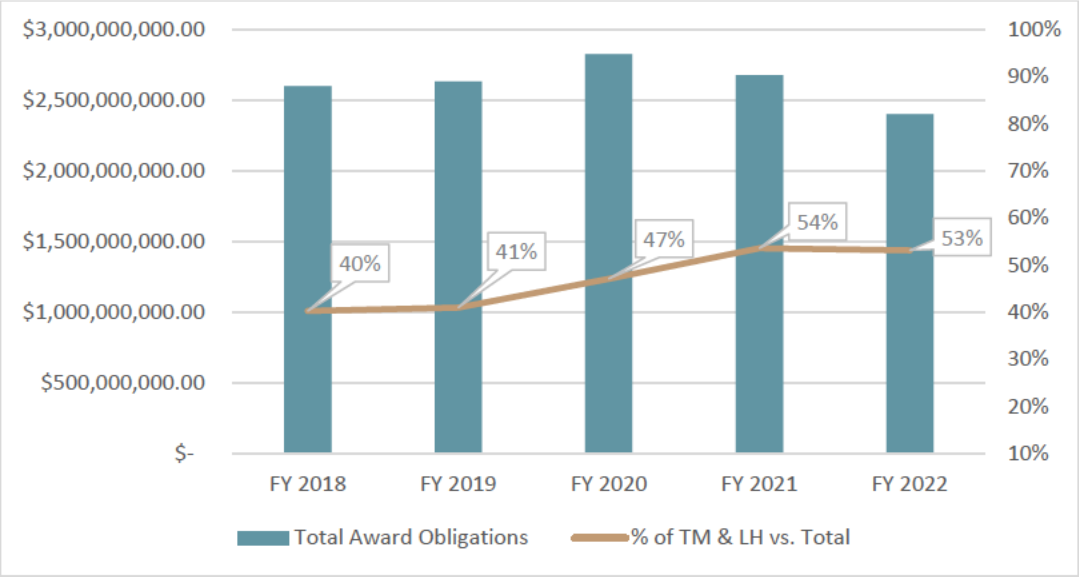
[56] As stated in Federal Acquisition Regulation 16.602, *Labor-hour contracts*, LH contracts are a variation of T&M contracts and differ only in that materials are not supplied by the contractor.

[57] U.S. Securities and Exchange Commission, *Fiscal Year 2021 Agency Financial Report*; November 15, 2021.

[58] We plan to initiate an audit of this issue in FY 2023.

[59] According to *usaspending.gov*, total (that is, cumulative) award obligations for all active SEC contracts as of October 7, 2022, was about $2.40 billion, of which total award obligations for T&M contracts was about $1.28 billion.

FIGURE 6. Percentage of SEC T&M Award Obligations Compared to Total SEC Award Obligations (FY 2018 – FY 2022)



Source: OIG-generated based on data retrieved from usaspending.gov on October 7, 2022.

As we have reported in prior years' statements on the SEC's management and performance challenges, Federal Acquisition Regulation Subpart 16.6, *Time-and-Materials, Labor-Hour, and Letter Contracts*, states, a T&M contract:

- ". . . provides no positive profit incentive to the contractor for cost control or labor efficiency."
- ". . . may be used only when it is not possible at the time of placing the contract to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence."

Furthermore, in June 2022, GAO reported that T&M and LH contracts are considered riskier than fixed price contracts because contractors bill the government by the hour and could conceivably work less efficiently so that they could charge more hours. As a result, GAO recommended that selected agencies assess steps they can take to use lower-risk contract types, and highlighted potential opportunities for agencies to assess ongoing use of T&M contracts in their acquisition portfolios.[60] Moreover, the Federal Acquisition Regulation encourages contracting officers to assess contract types periodically, after experience obtained during the performance of a T&M contract provides a basis for firmer pricing. A January 2021 OMB memorandum also discourages agency reliance on high-risk contracts, such as T&M contracts, stating that, "By managing contract types effectively, agencies have better leverage to ensure timely, efficient, and cost-effective completion of contractor work supporting critical and high priority goals."[61]

[60] U.S. Government Accountability Office, *Opportunities Exist to Reduce Use of Time-and-Materials Contracts* (GAO-22-104806, June 2022). GAO included in its review four Department of Defense agencies and field activities (the Air Force, Army, Defense Finance and Accounting Service, and Washington Headquarters Services), and three civilian agencies (the Social Security Administration, the Department of Homeland Security, and the Department of State).

[61] Office of Management and Budget, Memorandum M-21-11, *Increasing Attention to Federal Contract Type Decisions* (January 5, 2021).

Ongoing and Anticipated OIG Work. In FY 2023, we will continue to assess the SEC's contract management and acquisition processes through audits and evaluations and the work of our Acquisitions Working Group. We will complete an ongoing audit of the SEC's small business contracting program. In addition, we will assess the SEC's use of T&M contracts to help ensure such contracts are used only when appropriate and effective controls are in place to minimize the risk to the government. Lastly, we will report on any acquisition-related matters identified as a result of other ongoing and planned reviews of SEC programs and operations, and continue to support the SEC's efforts to train contracting officers and contracting officer's representatives about the potential for procurement-related fraud.

CHALLENGE: Ensuring Effective Human Capital Management

Although each component within the SEC is critical to achieving effective human capital management, the Office of Human Resources (OHR) is ultimately responsible for the strategic management of the SEC's human capital. OHR consults with management, establishes and administers human capital programs and policies, and ensures compliance with federal laws and regulations and negotiated agreements. It is critical that OHR develops and maintains the knowledge, skillsets, and expertise to guide the SEC through the challenges that inevitability arise in the management of a large professional workforce.

Indeed, retention, attrition, recruitment, and hiring of skilled personnel have all emerged as challenges within the SEC, along with the challenges associated with managing the agency's workforce throughout the COVID-19 pandemic.

Retention, Attrition, Recruitment, and Hiring

> *Effective management of an entity's workforce, its human capital, is essential to achieving results and an important part of internal control.*
>
> *Source: U.S. Government Accountability Office, Standards for Internal Control in the Federal Government (GAO-14-704G, September 2014), Principle 10 - Design Control Activities, section 10.03.*

The SEC recognizes the importance of an effective, highly-skilled, and diverse workforce. As such, in its strategic plan, the SEC states that it "will focus on recruiting, retaining, and training staff with the right mix of skills and expertise."[62] Moreover, Goal 1 of OHR's Human Capital Strategic Plan is to "Attract Diverse and Highly Talented People to the Agency."[63] OMWI also plays an important part in the agency's recruitment and retention efforts by providing leadership and guidance in ensuring diversity and inclusion with respect to the SEC workforce. In its Diversity and Inclusion Strategic Plan, the SEC highlights the importance of diversity, equity, and inclusion in the workplace, stating, "we recognize that our people are our most important asset. We also recognize that diversity, inclusion, and opportunity are essential to the agency's ability to effectively carry out its mission. These fundamental and value-enhancing tenets of our mission-oriented culture dictate that we continuously work to attract, hire, develop, and retain high-quality, diverse talent."[64]

Retention and Attrition

Despite OHR's and OMWI's efforts and the SEC being recognized as one of the best places to work in the federal government,[65] the SEC seems to be facing challenges to its retention efforts. As the figures below demonstrate, the SEC has seen a significant increase in attrition over the last few years, from 3.8 percent in FY 2020 to an estimated 6.4 percent in FY 2022 (as of September 20, 2022)—the highest attrition rate in 10 years. Most concerning is the increased attrition in Senior Officer and attorney positions, expected to be about 20.8 percent and about 8.4 percent for FY 2022, respectively.

---

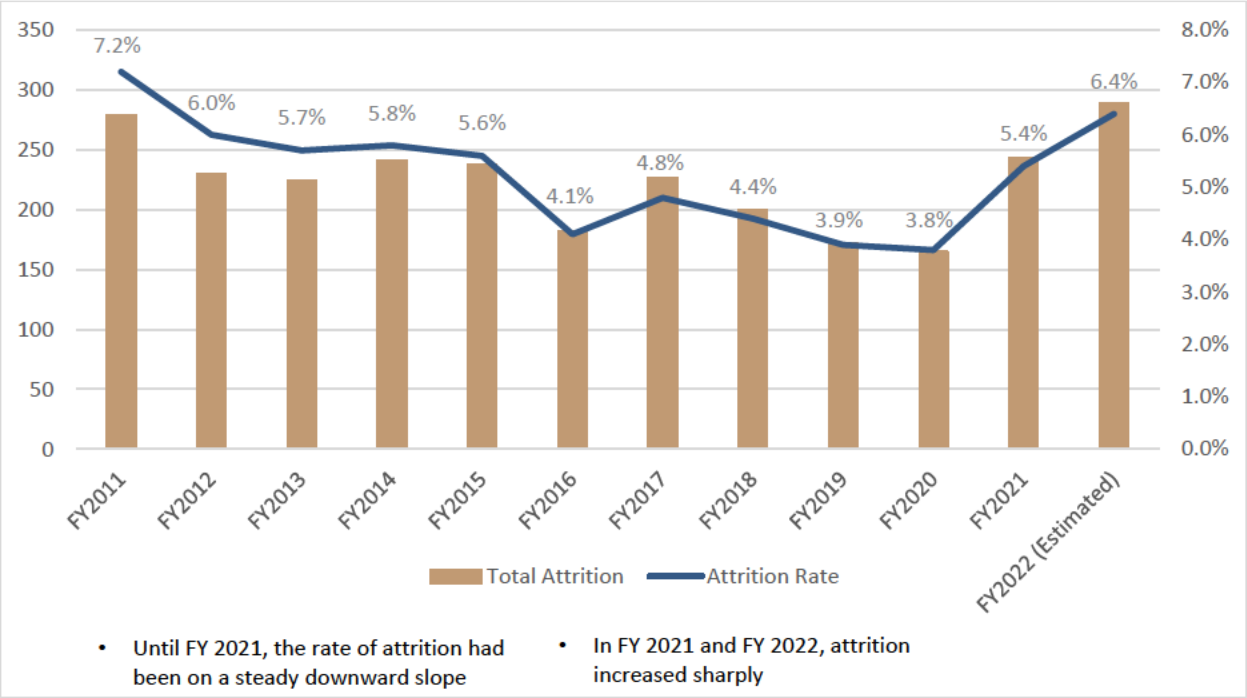
[62] U.S. Securities and Exchange Commission, *Strategic Plan Fiscal Years 2018-2022*, Strategic Initiative 3.1; October 11, 2018. The agency's draft strategic plan for FY 2022 to FY 2026 (Goal 3) similarly emphasizes the importance of attracting, hiring, developing, and retaining high-quality, diverse talent.

[63] U.S. Securities and Exchange Commission, Office of Human Resources, *FY 2020-2022 Human Capital Strategic Plan*; March 2020.

[64] U.S. Securities and Exchange Commission, *Diversity and Inclusion Strategic Plan*, Fiscal Years 2020-2022, Introduction.

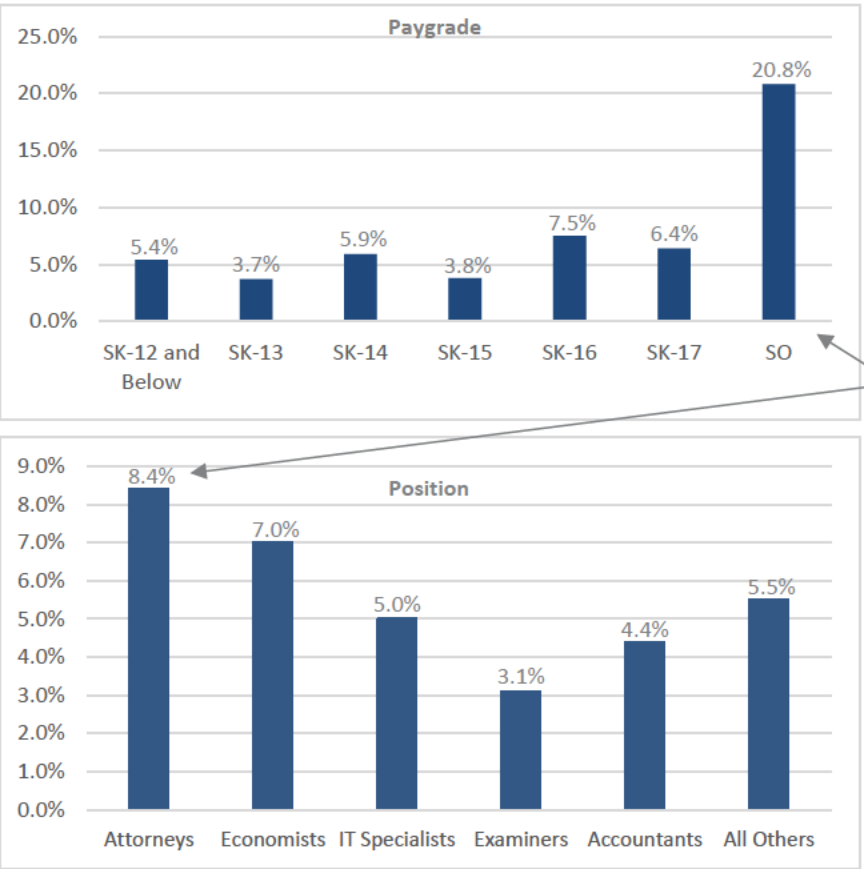
[65] Partnership for Public Service, *2021 Best Places to Work in the Federal Government Rankings*.

FIGURE 7. Total SEC Attrition (in Number of Positions) and Attrition Rate (FY 2011 – FY 2022)



Source: OIG-generated based on data provided by OHR.

FIGURE 8. SEC FY 2022 Expected Attrition by Paygrade and Position



In FY 2022, the greatest attrition was among SEC Senior Officers and attorneys

Source: OIG-generated based on data provided by OHR.

The SEC is not alone in facing a crisis to retain mission-critical talent during what has been dubbed "The Great Resignation." Critical elements of the federal workforce are in a state of stress. For example, according to the Partnership for Public Service, FY 2021 government-wide attrition rates averaged 6.1 percent, with certain groups experiencing even higher rates, such as women (6.4 percent) and executives (9.2 percent).[66]

The SEC may be able to address some of the concerns surrounding attrition by ensuring that it provides for succession planning through robust employee development and performance management. For example, in August 2022, the SEC launched a new program called LEAD (Leadership, Evaluation, Accession, and Development) to help SEC employees develop the leadership skills necessary to apply for future Senior Officer opportunities. However, performance management remains an area of opportunity for growth. For example, the SEC has discontinued the Performance Incentive Bonus program it implemented just 1 year ago. In addition, one recommendation from our 2018 report entitled, *The SEC Made Progress But Work Remains To Address Human Capital Management Challenges and Align With the Human Capital Framework,* remains open.[67] This recommendation—for the SEC to finalize standard operating procedures for the agency's performance management program—is an important component of the SEC's effort to ensure effective performance management. Agency management has reported that remediation work is underway, yet limited resources and competing priorities have created delays. In FY 2023, GAO is set to issue its triennial report on personnel management within the SEC,[68] which should provide further guidance to the SEC in this area.

Recruitment and Hiring

Recruitment is a major area of interest to both OHR and OMWI. Recruitment efforts are critical to ensuring a skilled and diverse candidate pool from which to fill SEC vacancies. In its FY 2023 Congressional Budget Justification, the SEC requested a total of 5,261 positions, an increase of 454 positions from FY 2022, in which the SEC was authorized 4,807 positions. With FY 2022 attrition rates estimated to be at 6.4 percent—or about 289 positions—efforts to recruit and hire an additional 454 new positions in FY 2023 could present challenges for OHR, OMWI, and SEC management. Moreover, the federal government is facing stiff competition from the private sector as increased wages and workforce engagement make private sector positions attractive to both new and seasoned professionals. The federal government hiring process also has been cited as a detriment when attracting talent to the federal government. For example, the federal government takes on average 98 days—more than twice as long as the private sector—to hire a new employee. [69] During our recent audit of the SEC's hiring process, discussed in more detail below, we found that of the 438 external hiring actions that we included in our analysis, nearly 50 percent took 100 business days or more to complete.[70]

---

[66] Partnership for Public Service. "Who Is Quitting and Retiring: Important Fiscal 2021 Trends in the Federal Government."

[67] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Made Progress But Work Remains To Address Human Capital Management Challenges and Align With the Human Capital Framework* (Report No. 549; September 11, 2018).

[68] Section 962 of Dodd-Frank includes a provision for GAO to report triennially on the SEC's personnel management, including the competence of professional staff; the effectiveness of supervisors; and issues related to employee performance assessments, promotion, and intra-agency communication. *See* Pub. L. No. 111-203, 124 Stat. 1376, 1908-1909 (2010) (codified at 15 U.S.C. § 78d-7).

[69] Partnership for Public Service. "Roadmap for Renewing Our Federal Government."

[70] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Can Improve in Several Areas Related to Hiring* (Report No. 572; February 28, 2022).

To address some of these recruitment concerns, OHR recently issued its FY 2022-2024 Recruitment and Outreach Strategic Plan, which identifies strategies to attract diverse talent and to aid in filling mission critical occupations that have been deemed hard-to-fill. Such strategies include creating branding and marketing that speaks to prospective applicants; developing and implementing a multi-media recruitment and agency branding campaign that highlights the successes of current SEC employees; developing a comprehensive internal communications strategy; and creating an overarching recruitment, outreach, and engagement tool to enhance the recruitment process.

Given the importance of an effective process when recruiting and hiring new employees, and the likelihood that the SEC will be heading into an intensive hiring effort, the OIG recently reviewed the SEC's hiring process and identified areas for improvement. The OIG's audit report, *The SEC Can Improve in Several Areas Related to Hiring*, addressed a number of critical areas related to the SEC's hiring process.[71] First, we determined that management can improve its controls to ensure Workforce Transformation and Tracking System (WTTS) data fields are accurate, consistent, and complete. We found that:

- 83 of the 91 hiring actions sampled (or about 91 percent) had at least one data entry issue in the WTTS data fields we reviewed, and almost 9 percent of the WTTS data entries we reviewed were either inaccurate, inconsistent, or incomplete;
- the SEC's WTTS data continued to include unannotated anomalies; and
- certain hiring actions were not consistently identified in WTTS.

These conditions occurred because (1) OHR's WTTS job aid did not include sufficient instructions regarding the dates and information expected in key WTTS data fields, and (2) some data fields were not included on the WTTS reports used by OHR staff to ensure the SEC's hiring action data was accurate, complete, and consistently recorded. As a result, OHR can further improve the reliability of the SEC's WTTS data to assist in workforce management and internal and external reporting of agency hiring information.

In addition, our assessment of OHR's quarterly Service Level Commitment (SLC) reviews found that (1) OHR did not perform SLC reviews in a consistent manner, (2) the review process was inefficient and prone to inaccuracies, and (3) SLC reviews did not align with the SLC presented to and agreed upon by the other SEC divisions and offices. This occurred because OHR did not establish clear guidance, including in the SLC itself, for the variety of hiring types and scenarios that can occur, or how to measure each one. The organization also did not ensure it could measure the SLC steps, as presented, in WTTS and did not effectively use the WTTS reporting capabilities in its SLC reviews. As a result, OHR limited its ability to rely on the SLC and SLC reviews as key controls for efficiently and effectively identifying areas of needed improvement in the SEC's hiring process, and for collaborating with the divisions and offices OHR serves.

Furthermore, we found that the SEC's pay-setting guidance needed improvement and OHR could clarify the new hire pay-setting information shared both internally and externally. Specifically, (1) the pay-setting

[71] Id.

information available to SEC employees and hiring officials was not comprehensive, (2) the internally published pay matrices were outdated, and (3) publicly advertised SEC salary information was misleading for new hires. We also identified inaccuracies in some of the underlying pay band information included in the 2021 pay matrices, and other pay-setting concerns. Incomplete, outdated, and misleading new hire pay-setting guidance and information have caused confusion and may have limited hiring officials' ability to review and respond to pay-setting requests. Although it does not appear that inaccurate information in the 2021 pay matrices impacted any newly hired SEC employee's pay, it could have had certain hiring scenarios occurred. We also concluded that OHR generally complied with the key hiring authority requirements tested; however, staffing case files for 18 of 32 attorney hiring actions we reviewed (about 56 percent) lacked supporting documentation, including proof of law degrees and/or bar membership. This occurred because OHR did not clarify review processes and documentation requirements for attorney qualifications. In addition, OHR's internal reviews of staffing case files needed improvement. As a result, the SEC risked hiring attorneys who did not meet all qualifications required for their position.

Lastly, we identified a matter that did not warrant recommendations related to (1) the SEC's SLC as compared to the Office of Personnel Management's end-to-end hiring process model timelines, and (2) feedback from the SEC divisions and offices OHR serves. We discussed this matter with agency management for their consideration.

We made 11 recommendations to further strengthen the SEC's controls over hiring actions, including recommendations to improve (1) the reliability of WTTS data, (2) assessments of the agency's hiring timelines, (3) the agency's compensation program, and (4) staffing case file documentation requirements. Management concurred with all 11 of our recommendations and, as of the date of this document, had taken action sufficient to close 5 of them. The remaining recommendations are open and will be closed by the OIG upon completion and verification of corrective action.

Responding to COVID-19: Workforce Perspectives

Responding to the COVID-19 pandemic has been a central concern of the SEC, and the federal government as a whole, throughout FY 2022. Since the outset of the national public health crisis and economic threats caused by COVID-19, the SEC's operational efforts have centered, first and foremost, on the health and safety of its employees, the employees and customers of its registrants, and individuals generally. From March 2020 through August 8, 2021, the SEC was in a mandatory telework posture, which aligned with other federal government agencies. Indeed, the federal government workforce quickly increased from 3 percent of employees teleworking every day to nearly 60 percent, as the 2020 Office of Personnel Management Federal Employee Viewpoint Survey shows.[72] However, as vaccines became more widely available, the SEC shifted its focus to how to best and most safely allow employees to return to the workplace.

[72] Office of Personnel Management, *Government-wide Management Report: Results from the 2020 OPM Federal Employee Viewpoint Survey*; April 26, 2021.

Safety remains a top priority when planning for employee return to the workplace

On August 9, 2021, the agency began to allow vaccinated employees to voluntarily return to the workplace. In calendar year 2022, peak occupancy across all SEC building locations has averaged around 7 percent. The SEC has not yet mandated that its employees return to the office in pre-COVID-19 levels. On July 25, 2022, the agency announced that, because of the recent uptick in COVID-19 community levels, the planned return-to-office date was shifted from September 6, 2022, to January 9, 2023. Occurring alongside the agency's monitoring of community levels, the SEC is also negotiating a new collective bargaining agreement with the National Treasury Employees Union, which will include updated provisions related to telework and remote work. The parties are also engaged in bargaining related to the mandatory return-to-office plan. While these negotiations are ongoing, both the National Treasury Employees Union and SEC leadership make regular announcements to staff and management, respectively, about their progress. At this point, further negotiations require assistance from the Federal Mediation and Conciliation Service as the parties endeavor to avoid invoking the Federal Services Impasse Panel for a final decision on the terms of the new collective bargaining agreement and return-to-office plan. The uncertainty surrounding the plans for return-to-office and the potential for expanded telework and/or workplace flexibilities makes it more difficult to plan for future human capital management solutions.

Ongoing and Anticipated OIG Work. In FY 2023, we plan to evaluate the agency's workplace safety protocols developed in response to the COVID-19 pandemic, including the COVID-19 workplace safety plan and related measures, such as those established pursuant to OMB Memorandum M-21-15, Executive Order 13991, and other applicable guidance. We also will complete a review of the agency's upward mobility program. Furthermore, we will monitor the SEC's progress in addressing prior open audit recommendations related to human capital management. To assess the SEC's efforts to promote diversity, equity, inclusion, accessibility, and opportunity, we will complete an ongoing audit of the agency's small business contracting. We will also assess the operations and controls over the agency's equal employment opportunity program.

OIG General Office Contact Information

EMPLOYEE SUGGESTION PROGRAM

The OIG SEC Employee Suggestion Program, established under the Dodd-Frank Wall Street Reform and Consumer Protection Act, welcomes suggestions by all SEC employees for improvements in the SEC's work efficiency, effectiveness, productivity, and use of resources. The OIG evaluates all suggestions received and forwards them to agency management for implementation, as appropriate. SEC employees may submit suggestions by calling (202) 551-6062 or sending an e-mail to OIGESProgram@sec.gov.

COMMENTS AND IDEAS

The SEC OIG also seeks ideas for possible future audits, evaluations, or reviews. We will focus on high-risk programs, operations, and areas where substantial economies and efficiencies can be achieved. Please send your input to AUDPlanning@sec.gov.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees, or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

CONTACT US BY MAIL AT

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