NASA OFFICE OF INSPECTOR GENERAL

SUITE 8U71, 300 E ST SW
WASHINGTON, D.C. 20546-0001

February 1, 2024

The Honorable Jeanne Shaheen
Chairwoman
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Jerry Moran
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Harold Rogers
Chairman
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

The Honorable Matthew Cartwright
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Subject: *NASA's Compliance with Federal Export Control Laws* (IG-24-007)

The National Aeronautics and Space Administration (NASA) Authorization Act of 2000 directs the NASA Office of Inspector General (OIG) to annually assess the Agency's compliance with federal export control laws and reporting requirements regarding cooperative agreements between NASA and China or any Chinese company.[1]

We last reported to you on these issues in February 2023. Since then, NASA has not established any new bilateral agreements with China. NASA has continued its work with the Chinese Academy of Sciences on bilateral science activities relating to space geodesy and glacier research in the Himalaya Region.[2] In June 2021, NASA began to exchange limited information with the China National Space Administration (CNSA) to ensure the safety of NASA's robotic Mars science missions and international

[1] Pub. L. No. 106-391, codified at 51 U.S.C. § 30701(a)(3).

[2] Space geodesy uses space-based observations to monitor, map, and understand changes in the Earth's shape, rotation, and mass distribution.

partners' missions in orbit around Mars. NASA anticipates these discussions will continue for the life of the Tianwen-1 mission.[3] Additionally, according to Agency officials, in November 2023 NASA permitted NASA-funded scientists to apply for access to CNSA's Chang'e-5 lunar samples.[4] As of January 2024, discussions are ongoing within the Agency regarding terms for the exchange of the samples and the process for engaging with CNSA. For each of these activities, the Agency made the appropriate notifications in accordance with the requirements outlined in Public Law 116-260.[5]

With regard to export control-related oversight work conducted by our office, during the past year we completed one audit related to NASA's partnerships with international space agencies for the Artemis campaign and three audits that examined NASA's controls over sensitive information and information technology (IT) assets and security systems, many of which contain data subject to export control laws. We also initiated two new audits related to IT security. In addition, our Office of Investigations closed nine investigations related to inappropriate associations with China and the unauthorized access to export-controlled information. Furthermore, we are an active member of the U.S. Department of Homeland Security's Export Enforcement Coordination Center (E2C2). The E2C2 coordinates export enforcement efforts and intelligence sharing activities among federal agencies to identify and resolve conflicts involving violations of U.S. export control laws.

We summarize our 2023 export control and IT security systems audits and investigations below.

AUDIT REPORTS ISSUED

NASA's Partnerships with International Space Agencies for the Artemis Campaign (IG-23-004, January 17, 2023)

NASA's Artemis campaign is working toward landing humans on the Moon in 2025 with the ultimate goal of crewed missions to Mars in the 2030s. Additional objectives include robotic and scientific missions to the lunar surface, establishing an orbiting lunar outpost known as Gateway, and developing a base camp with lunar rovers on the Moon. Achieving these ambitious objectives is both technically challenging and enormously expensive, with NASA's financial contributions to Artemis projected to cost $93 billion between fiscal years 2012 and 2025. Consequently, NASA officials have stated that partnerships with international space agencies are critical to achieving the Artemis campaign's goals. The Artemis Accords—signed by 23 countries over the last 2 years—illustrate wide international interest in space exploration as they seek to establish principles for cooperation among civil space agencies and governance on increasing the safety of operations, reducing uncertainty, and promoting the sustainable and beneficial use of space.

---

[3] Tianwen-1 is an interplanetary mission by the China National Space Administration that launched in July 2020 and landed a rover on Mars in May 2021.

[4] In December 2020, China's Chang'e-5 lunar mission returned to Earth after retrieving lunar rocks and soil.

[5] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260 (2020) requires NASA to certify to the Senate and House committees on appropriations and the Federal Bureau of Investigation (FBI) no later than 30 days prior to the event that the activities pose no risk of a transfer of technology, data, or other information with national security or economic security implications and that the activities will not involve knowing interactions with officials who have been determined to have direct involvement with violations of human rights.

Key early Artemis commitments from the Canadian Space Agency, European Space Agency, and Japan Aerospace Exploration Agency include the provision of a Gateway habitat, communications satellites, spacecraft service modules, external robotics, astronauts, and lunar rovers. NASA is leaning into 30 years of experience working with a variety of international partners on the International Space Station (ISS) by establishing long-term Artemis commitments from many of the same partners, but international cooperation for Artemis may be hindered by fluctuating political guidance, uncertain budgets, and restrictive policies concerning the control of mission-related information both in the United States and abroad. In this audit we evaluated (1) NASA's plans to coordinate and integrate international partner contributions with its Artemis efforts, (2) impediments NASA faces when partnering with international space agencies, and (3) the cost implications of working with partner space agencies.

Interest in the Artemis campaign is high across the international space community, as evidenced by NASA's 54 Artemis-related international instruments and the 23 signatories to the Artemis Accords. However, the Agency lacks an overarching strategy to coordinate Artemis contributions from international space agencies and entities. Except for the Gateway Program, the Artemis campaign lacks comprehensive forums—boards, panels, and working groups— for its international partners to routinely discuss topics such as flight and mission planning, safety, and research integration. In contrast, the ISS Program—seen as a model of long-term international space cooperation—employs these forums as well as on-site representation from partner agencies. While the blueprint for the first three Artemis missions is well established, NASA lacks an overall blueprint beyond Artemis IV for lunar exploration of the Moon that includes estimated costs and the responsibilities of its international partners. In May 2022, NASA took steps to develop a "blueprint for sustained human presence throughout the solar system," but it is too early to tell if these efforts will clarify the potential funding, roles, and responsibilities required of international partners participating in the Artemis campaign. Additionally, current Artemis agreements are pursued bilaterally with interested parties, without an overall cooperative framework that addresses the legal structure, program development, or partner roles and responsibilities.

U.S. export control regulations of defense articles and commercial items—governed by rules known as the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)—are designed to protect U.S. national interests and intellectual property. However, they can be overly complex and restrictive, and their implementation in international agreements, policies, and space flight system classification routinely limit NASA's international collaborations on Artemis. For example, international agreements do not allow the use of partner astronauts or sharing information with them during the periods prior to and after conclusion of a mission. In addition, unlike the ISS, the Artemis campaign lacks a unique EAR classification of specific space flight items or consistent jurisdiction and classification of Artemis elements, such as the Orion spacecraft, that would simplify the timely exchange of space flight items and technical information with international partners.

With costs for the Artemis campaign likely to reach hundreds of billions of dollars over the next two decades, NASA is trying to make its Moon to Mars plans more sustainable by sharing costs with its international partners. Partners are helping to defray costs by providing a capability—such as space flight hardware and related operations, robotics, or enhanced lunar communication—with the value for that capability determined at the outset of the agreement, rather than allocating a specific percentage of costs to each partner or creating an ongoing obligation to include partner astronauts on future missions. Our analysis showed that uncrewed and robotic space flight projects in which NASA works with international partners have, on average, experienced less cost growth despite higher levels of complexity. NASA's international partners use trade studies to understand potential costs and technical

requirements early in a project, allowing for use of firm-fixed-price contracts that aid in controlling project costs. Given NASA's deep space ambitions and current budget profile, the Agency will be unable to achieve its long-term Artemis objectives without effectively incorporating international partner cost-management strategies.

We made 10 recommendations to increase the effectiveness and affordability of Artemis integration efforts with international partners; NASA concurred with nine, one is now closed, and the Agency is planning to implement corrective action for the others by March 2024. The Agency non-concurred with one recommendation, and it remains unresolved pending further discussions.

To view the full report, visit NASA's Partnerships with International Space Agencies for the Artemis Campaign.

NASA's Software Asset Management (IG-23-008, January 12, 2023)

NASA uses thousands of unique software products from hundreds of vendors in its efforts to advance science, technology, aeronautics, Earth studies, and space exploration. Each software application and program comes with a license—a contract between the entity creating or supplying the software and the end user—governing its use. Managing software licensing is deceptively complex due to the sheer volume of software vendors and applications, yet it is crucial to effectively secure NASA operations and track tens of millions of dollars in license fees. Software asset management is the business practice that administers the processes, policies, and procedures that support the software life cycle of planning, acquisition, use, management, and disposal.

Effective software asset management helps reduce IT costs and mitigate operational, cybersecurity, and financial risks related to software ownership and use. NASA's software portfolio consists of purchased software programs subject to varying types of licenses as well as internally developed mission and institutional software applications that are not licensed by the Agency. Purchased software must be used in accordance with the terms of its license with potential financial penalties if vendor audits find violations of license agreements. Internally developed software also needs to be tracked to identify duplicate or obsolete applications.

In this audit, we assessed whether NASA is managing its software assets in an effective and efficient manner while maintaining compliance with applicable requirements and security best practices.

Software asset management practices at NASA currently expose the Agency to operational, financial, and cybersecurity risks with management of the software life cycle largely decentralized and ad hoc. Efforts to implement an enterprise-wide software asset management program have been hindered by both budget and staffing issues and the complexity and volume of the Agency's software licensing agreements. We rated NASA's software asset management as "basic"— the lowest of the four rating options in the Software Asset Management Maturity and Optimization Model developed by Microsoft and adopted from the International Organization for Standardization/International Electrotechnical Commission. Consequently, NASA is likely years away from moving to an enterprise computing model in which IT capabilities, such as software asset management and cybersecurity, are centralized and consolidated. In the meantime, the Agency has yet to embrace key best practices or fully implement federal guidance required to appropriately manage its software asset management program.

NASA has not implemented a centralized software asset management tool to discover, inventory, and track license data as required by federal policy. This shortcoming has resulted in NASA spending approximately $15 million over the past 5 years on unused licenses, an amount we found wasteful and therefore questioned. We also found internally developed mission and institutional software applications suffer from a lack of centralization and inventory visibility, limiting the Agency's ability to identify duplicative or obsolete software. NASA's software asset management policy is not comprehensive or standardized, leaving roles, responsibilities, and processes unclear. In addition, the Agency's Software Asset Management Office and Software Manager positions are misaligned and do not report to the Chief Information Officer as required by federal policy. The Agency also does not have consistent processes for legal representation during software contract negotiations and vendor audits, which can expose the Agency to increased costs because of penalties for violations of software license agreements. Furthermore, training for software license use and management is inconsistent across the Agency, with aging web-based training randomly assigned and a lack of general software licensing training available to the entire workforce.

NASA has failed to implement processes necessary to manage financial risks as software purchases are not sufficiently tracked and authorized by the Office of the Chief Information Officer (OCIO)—allowing some users to bypass OCIO authorization (and Software Asset Management team scrutiny) to purchase software through alternative means such as purchase cards. Moreover, NASA's current efforts to compile a complete and accurate report of annual software spending is a time consuming and mostly manual effort. Given these shortcomings, NASA has historically experienced a large influx of software into its network environment that is not sufficiently tracked for license compliance, resulting in more than $20 million unnecessarily spent on software fines and penalties over the last 5 years. We estimate the Agency could have saved approximately $35 million ($20 million in fines and overpayments and $15 million in unused licenses) and, moving forward, could save $4 million over the next 3 years by implementing an enterprise-wide software asset management program.

Lastly, NASA has not implemented the enterprise-wide processes necessary to appropriately manage software asset management cybersecurity risks. Software downloaded with privileged access is not tracked for license compliance and life-cycle management, and NASA does not have a consistent, Agency-wide process for giving users only the software permissions necessary for their job. This deviation from best practices is a cybersecurity risk because software deployed within the Agency raises both cybersecurity and software license compliance risks.

We made nine recommendations to strengthen operational and cyber aspects of software asset management; the Agency concurred or partially concurred with all of them. Four of the nine recommendations are now closed, and the Agency plans to implement corrective action for four of the remaining by October 2024. Corrective action for the final recommendation is planned to be completed by October 2027.

To view the full report, visit NASA's Software Asset Management.

NASA's Management of Its Artificial Intelligence Capabilities (IG-23-012, May 3, 2023)

Artificial intelligence (AI) is generally thought of as the capability of a machine to imitate intelligent human behavior. Aspects of this technology are used in a wide variety of applications from medical devices to autonomous vehicles, with tools like ChatGPT capable of mimicking human thought processes. NASA is a leader in AI usage and innovation across government, with applications such as a

storm prediction tool that uses image recognition technology to identify atmospheric conditions to provide early warnings for destructive hailstorms and space vehicles such as the Mars Perseverance rover that uses an autonomous navigation system. While NASA and other federal agencies are continually exploring ways to incorporate AI into their organizations to meet agency goals, its adoption across such a wide spectrum of disciplines raises challenges for regulating and managing risks such as cybersecurity threats and drives the need for more detailed federal governance.

To that end, in February 2019 the White House issued Executive Order (EO) 13859 to promote sustained investment in AI research and development to generate technological breakthroughs while bolstering the requirement for AI developers to minimize vulnerability to attacks from malicious actors and reflect federal priorities for innovation, public trust, and public confidence in AI systems. Similarly, EO 13960, issued in December 2020, seeks to promote the continued expansion of AI research and development in the United States while introducing measurable requirements to promote transparency and trustworthiness. Although these EOs establish baseline principles for agencies to adopt into their AI governance policies and practices, AI standards remain in their infancy across the federal government.

In this audit we examined NASA's progress in developing its AI governance framework and standards and assessed whether security controls are being considered and implemented to protect AI data and technologies from cyber threats.

NASA has made progress in establishing an AI framework through development of the NASA Framework for the Ethical Use of Artificial Intelligence in April 2021, which drew upon the principles of leading AI organizations to guide consideration of ethics for AI projects and provide initial recommendations for NASA governance, advice related to AI, and questions for AI practitioners to consider during their work. Additionally, development of NASA's Responsible AI Plan in September 2022 identified NASA's responsible AI officials and outlined how NASA intends to implement requirements of EO 13960, including capturing and reporting use-case inventories, establishing oversight of AI projects to ensure continuous monitoring efforts, and engaging the AI community on the Agency's ethical AI standards and how to implement them.

However, NASA has not adopted a standard definition of AI and instead has three separate definitions: one in the NASA Framework for the Ethical Use of Artificial Intelligence, one in NASA's Responsible AI Plan that utilizes the definition found within EO 13960, and one on NASA's internal Artificial Intelligence Machine Learning SharePoint collaboration website. While all three definitions are similar, subtleties and nuances in each can alter whether a particular technology is properly considered AI. Personnel we interviewed stated they reported AI based on their own individual understanding of what the term means rather than a formal definition provided by the Agency. As a result, NASA does not have a singular designation or classification mechanism to accurately classify and track AI or to identify AI expenditures within the Agency's financial system, making it difficult for the Agency to meet federal requirements to monitor its use of AI. Moreover, at NASA AI is generally managed as part of a larger project rather than as its own project and therefore is not tracked separately. This impacted the Agency's response to EO 13960 to create an AI inventory as well as its response to EO 13859 to compile an estimated annual budget for AI expenditures. To compile such an inventory and budget, NASA uses a multi-faceted data call to gather individual responses from AI users, which takes significant time to compile, validate, and vet and runs the risk of clerical errors that could be significantly lessened using an automated process.

Further, EO 13859 requires that technical controls exist to minimize AI's vulnerability to attack by a malicious actor. Agency officials believe NASA's existing processes should be adequate to address security concerns specific to AI including monitoring requirements and ensuring NASA's AI is properly safeguarded from cybersecurity vulnerabilities. However, our prior work has shown that NASA's fragmented approach to IT management puts the Agency at a higher-than-necessary risk from cyber threats. Without an AI-specific classification mechanism or means to appropriately categorize and classify AI within its system of records, the Agency faces increased challenges to implement potential future federal AI cybersecurity controls.

We made four recommendations to improve the governance, budgeting, and cybersecurity of NASA's AI capabilities; the Agency concurred or partially concurred with all of them. One recommendation is now closed, and the Agency plans to implement corrective action for the remaining by July 2024.

To view the full report, visit NASA's Management of Its Artificial Intelligence Capabilities.

NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023 (IG-23-017, August 17, 2023)

The Federal Information Security Modernization Act of 2014 (FISMA) requires the OIG, or an independent external auditor, to conduct an annual evaluation of NASA's information security program. The OIG selected the independent public accounting firm RMA Associates, LLC (RMA) to evaluate NASA's information security program in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* and against the fiscal year 2023 Inspector General FISMA Reporting Metrics (IG Metrics). The evaluation rated NASA's information security program at a Level 3 (Consistently Implemented), which means policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking. This rating fell short of the Office of Management and Budget's rating that agency cybersecurity programs should be considered effective.

RMA determined the maturity level for all five cybersecurity functions (Identify, Protect, Detect, Respond, Recover) using a calculated average scoring model based on testing of the fiscal year 2023 core and supplemental metrics. The Identify, Detect, and Recover functions were rated at a Level 2 (Defined) while the remaining two functions were rated at a Level 3 (Consistently Implemented).

For the Identify function, information contained in NASA's Risk Information Security Compliance System—the system of record for information systems—was not current. Specifically, two systems selected for testing were listed as operational but were not in use. Additionally, one of the systems selected for testing could not provide evidence to demonstrate an up-to-date inventory of all licenses used within its system boundaries. The Agency also did not have policies, procedures, and processes for risk framing, response, and risk monitoring to manage cybersecurity risks. Further, NASA did not complete the development of an enterprise-wide risk register or a risk profile to record, track, and communicate enterprise-wide cybersecurity risk management data to support enterprise-level decision-making and activities across the Agency.

NASA has not incorporated enterprise-wide supplier risk evaluations into the Agency's continuous monitoring practices. Additionally, while NASA has begun the process of developing its Cybersecurity Supply Chain Risk Management controls and has made measurable progress in developing and

implementing its supply chain risk management processes across the Agency, NASA had not completed these efforts.

For the Detect function, NASA did not have a formal process to document and implement information security and continuous monitoring lessons learned to improve its existing control effectiveness. NASA's information security and continuous monitoring strategy was not updated in accordance with the latest federal requirements. Finally, for two of the four systems selected for testing, the Authorization to Operate was not up to date and the system-level security assessment report was not updated continuously or annually.

Lastly, for the Recover function, one system selected for testing did not perform a business impact analysis, which analyzes the system's requirements, functions, interdependencies, and priorities to minimize the impact of an event of significant disruption. NASA lacks centralized IT governance procedures or oversight to monitor and enforce business impact analyses compliance at the system level. In addition, NASA did not implement the necessary oversight mechanisms and controls to ensure all system-level contingency plans were developed, tested, and results reviewed to develop corrective actions as needed. Contingency plans for two information systems were not tested as required by NASA policy. Finally, an external information system did not have the appropriate agreement in place to specify the technical and security requirements of the interconnection of the system with its external system partner.

RMA made 27 recommendations to address deficiencies across all 5 functions. NASA concurred with all recommendations and plans to take correction action by July 2024.

To view the full report, visit NASA's Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2023.

ONGOING AUDIT WORK

Audit of NASA's High-End Computing Program

NASA's High-End Computing Program provides computing systems and services to support the Agency's aeronautics, exploration, science, and space technology missions. High-end computing enables scientists and engineers to model and analyze data up to 10 times faster and view results at a higher fidelity. This audit will assess NASA's management of its High-End Computing Program, specifically the Agency's processes and controls related to the Program's policy framework, capacity planning, stakeholder engagement, and cybersecurity.

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2024

Required by the Federal Information Security Modernization Act of 2014, the Office of Inspector General is conducting the fiscal year 2024 evaluation of NASA's information security program and will report the results to the Office of Management and Budget.

INVESTIGATIONS

3D Printing Company Agrees to Civil Settlement

The U.S. Attorney's Office for the Northern District of Texas reached a civil settlement with a Texas 3D printing company that agreed to pay the United States up to $4.54 million to resolve allegations that it violated the False Claims Act by improperly transmitting export-controlled NASA and U.S. Department of Defense technical data to a company in China. The potential full settlement amount includes $2.27 million in restitution and an additional $2.27 million in penalties should the company fail to pay the same amount to the U.S. Department of State and U.S. Department of Commerce in connection with a parallel administrative settlement.

Contractor Agrees to Settle False Claims Allegations

As the result of a joint investigation by the NASA OIG, Air Force Office of Special Investigations, and Defense Criminal Investigative Service, a Colorado laser manufacturer agreed to a civil settlement of $402,621 to settle allegations that it used foreign employees to conduct research and development consulting services without government approval.

University Agrees to Civil Settlement

As the result of a joint investigation by the NASA OIG, Federal Bureau of Investigation (FBI), U.S. Army Criminal Investigation Division, and National Science Foundation OIG, an Ohio university agreed to a civil settlement of $875,689 to resolve allegations that it failed to disclose a professor's affiliations with and support from a foreign government in connection with research funding from NASA and other federal agencies.

Former NASA Contractor Sentenced for Export Violation

A former NASA contractor employee pled guilty to illegally transferring flight control software to a university in the People's Republic of China. As a result, he was sentenced to 20 months of confinement, followed by 3 years of supervised release, and ordered to pay $168,885 in restitution. This was the result of a joint investigation by the NASA OIG, Army Criminal Investigation Division, FBI, Defense Criminal Investigative Service, and Department of Commerce Office of Export Enforcement.

University of Arkansas Professor Debarred

A University of Arkansas professor was debarred for a period of 5 years for making a false statement to the FBI regarding the existence of patents issued by the People's Republic of China for his inventions. The professor was previously sentenced to 12 months of imprisonment for this action, followed by 12 months of supervised release, and ordered to pay a $5,000 fine.

Former University Professor Debarred for 3 Years

A former Texas A&M University professor was debarred for 3 years for failing to disclose his association with entities in China while receiving NASA grant funds.

Unauthorized Release of Software to a Foreign Entity

A NASA OIG investigation revealed the unauthorized release of flight termination software to a foreign entity in New Zealand by two NASA contractors, one of whom was a former NASA civil servant. While the case was declined for prosecution, NASA's Acquisition Integrity Program addressed the flawed software process that allowed the unauthorized release.

Hubble Space Telescope Export-Controlled Material Posted for Sale

Several presentations related to the Hubble Space Telescope project marked as export controlled under ITAR were posted on eBay for sale. The items may have originated from an estate sale of a deceased NASA employee. As a result of the OIG investigation, the items were removed from the website, and the seller was educated on the implications of selling export-controlled documents to foreign nationals and the need to coordinate with NASA export control officials in the future.

Orion Space Vehicle ITAR Documents Seized

In July 2023, NASA OIG seized three documents on the Orion spacecraft from an eBay retailer in Cocoa, Florida. The documents were ITAR controlled and returned to the Kennedy Space Center Export Administrator. The case was declined for prosecution.

If you or your staff have any questions or would like further information on any of the audit reports or investigations discussed in this letter, please contact me or Renee Juhans, OIG Executive Officer, at 202-358-1220 or renee.n.juhans@nasa.gov.

George A. Scott
Digitally signed by George Scott
Date: 2024.01.31 11:56:32 -05'00'

George A. Scott
Acting Inspector General

cc: Bill Nelson
Administrator

Pamela Melroy
Deputy Administrator

James Free
Associate Administrator

Bale Dalton
Chief of Staff

Jeff Seaton
Chief Information Officer

Iris Lan
General Counsel

Karen Feldstein
Associate Administrator for International and Interagency Relations

Robert Gibbs
Associate Administrator for Mission Support Directorate

Enclosure—1

ENCLOSURE I: CONGRESSIONAL RECIPIENTS

United States Senate

Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Commerce, Science, and Transportation
Committee on Homeland Security and Governmental Affairs

U.S. House of Representatives

Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Oversight and Accountability
Committee on Science, Space, and Technology