

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6375

www.science.house.gov

May 27, 2021

Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Dodaro:

The National Aeronautics and Space Administration (NASA) is planning to invest at least \$65 billion over the life cycle of its current portfolio of 25 major space development projects. NASA's portfolio of major projects includes satellites equipped with advanced sensors to study the Earth, telescopes intended to explore the universe, and spacecraft to transport humans and cargo beyond low-Earth orbit. As each project represents significant investments in innovative technology, they could also be attractive targets to malicious actors. In particular, each project has sensitive data relating to, among others, intellectual property and safety-related flight systems. In addition to development, NASA and its partners operate spacecraft and carry out services, including launching cargo and crew to the International Space Station.

Cyber-based threats to the sensitive data associated with NASA's major space projects can come from multiple threat actors (e.g., nations, insiders, criminal organizations) and can have significant adverse impacts. For example, in December 2018, a grand jury in the United States District Court for the Southern District of New York indicted two Chinese hackers associated with the Ministry of State for computer intrusions targeting, among many others, sensitive technology data maintained at NASA's Goddard Space Center and Jet Propulsion Laboratory.¹ Similarly, the U.S.-China Economic and Security Review Commission's 2011 annual report

¹United States District Court for Southern District of New York. (2018) *United States v. Zhu Hua, a/k/a/"Afwar," a/k/a "CVNX," aka "Alayos," a/k/a "Godkiller," and Zhang Silong, a/k/a "Baobeilong," a/k/a Zhang Jianguo," a/k/a "Atreexp."* Dec. 17 file date. <https://www.justice.gov/opa/press-release/file/1121706/download>.

highlighted “at least two U.S. government satellites have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems.”² In addition, according to NASA’s Office of the Inspector General (OIG), potential infiltration into NASA’s space flight systems to acquire launch codes and flight trajectories of spacecraft remains a particular concern of NASA’s information technology (IT) security managers.³

NASA also shares responsibility with its contractors for protecting the agency’s sensitive data from cyber threats; however, NASA’s OIG has previously identified weaknesses in the agency’s processes for overseeing its contractors’ cybersecurity practices. For example, in June 2019, NASA’s OIG reported that NASA did not explicitly include security event and incident data sharing or oversight requirements in the 5-year contract it signed with the California Institute of Technology in October 2018 for the operations of the Jet Propulsion Laboratory.⁴ More recently, other agencies, particularly the Department of Defense, have recognized the increasing cyber threat to the contractors supporting agency projects and systems and have taken steps to provide increased assurance that contractors are adequately addressing this threat. For example, the Department of Defense will soon begin implementing its Cybersecurity Maturity Model Certification program, which will be used to verify the extent to which the Department’s contractors have implemented appropriate cybersecurity practices.

GAO and NASA’s OIG have reported on longstanding weaknesses in NASA’s processes for addressing cybersecurity threats.⁵ The extent to which these ongoing weaknesses have impacted the agency’s ability to protect its most sensitive data, especially data tied to its major space development projects and spacecraft and human spaceflight operations, is not well understood. Recent, sophisticated cybersecurity attacks on multiple Federal government systems that went undetected for months underscore the importance of having robust processes in place manage cybersecurity risks related to NASA’s sensitive data.

As NASA continues to lead the nation and the world in pursuing ambitious goals, including human exploration of the Moon and Mars and ever more challenging scientific investigations, it is imperative that it do so in a manner that protects sensitive data from malicious actors. Accordingly, we request that GAO conduct a review of the cybersecurity risks to the sensitive data associated with NASA’s major projects and spaceflight operations. In formulating its specific objectives for this work, we ask that GAO:

² U.S.-China Economic and Security Review Commission, *2011 Report to Congress* (November 2011) https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

³ NASA Office of Inspector General, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory*, IG-19-022 (June 18, 2019).

⁴Id.

⁵GAO, *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, GAO-18-337 (Washington, D.C. May 22, 2018); *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009); Office of Management and Budget, *Federal Information Security Modernization Act: Annual Report to Congress Fiscal Year 2019*.

- (1) compare NASA's efforts to protect the sensitive data associated with its major projects from cyber threats with leading cybersecurity practices, including those practices needed to establish accountability for the effective implementation of cybersecurity controls;
- (2) assess the extent to which the contracts for select NASA major projects include cybersecurity requirements that are consistent with best practices;
- (3) identify further actions that NASA could take in working with its contractors and service providers to strengthen cybersecurity and protect sensitive data;
- (4) review NASA's coordination with other agencies in the federal government tasked with cybersecurity and industrial information system security responsibilities, the effectiveness of NASA's implementation of existing interagency agreements, NASA's policies, procedures, and authorities, as they compare to other relevant federal agencies; and
- (5) evaluate NASA's compliance with existing policies, standards, best practices, and controls for overseeing contractor cybersecurity and protection of government-funded sensitive data.

Please contact Ms. Pamela Whitney, Majority Committee staff at (202) 225-6375 and Mr. Tom Hammond, Minority Committee Staff at (202) 225-6371 to discuss the details and timing of this GAO review.

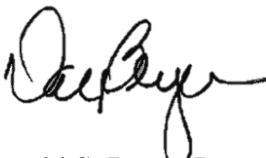
Sincerely,



Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology
Technology



Frank Lucas
Ranking Member
Committee on Science, Space, and



Donald S. Beyer Jr.
Chairman
Subcommittee on Space and Aeronautics



Brian Babin
Ranking Member
Subcommittee on Space and Aeronautics