SUBCOMMITTEE ON SPACE AND AERONAUTICS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

HEARING CHARTER

Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19

September 18, 2020
11:00 a.m.
Cisco WebEx

PURPOSE

The purpose of the hearing is to examine the status of NASA's cybersecurity and information technology management, policies, and practices, including cybersecurity challenges associated with increased telework and remote operations during the COVID-19 pandemic, and other issues.

WITNESSES

- **Mr. Jeff Seaton,** Chief Information Officer (Acting), National Aeronautics and Space Administration
- **The Honorable Paul K. Martin,** Inspector General, National Aeronautics and Space Administration
- **Diana L. Burley, PhD,** Vice Provost for Research, American University

OVERARCHING QUESTIONS

- *What are the implications of cybersecurity vulnerabilities to NASA's mission and operations?*
- *How has the coronavirus pandemic, and the associated increase in and extended duration of telework, affected NASA's cybersecurity vulnerabilities, and to what extent has NASA addressed any changing risks?*
- *Why have the NASA Inspector General and the Government Accountability Office consistently listed cybersecurity as a top challenge for NASA, and what progress has NASA made to address the Agency-wide cybersecurity challenges?*

BACKGROUND

The National Aeronautics and Space Administration (NASA), as any federal government agency, makes widespread use of information technology (IT) and associated systems and services, and needs to protect its systems from unauthorized access and malicious activities. The risks to IT systems supporting the federal government are increasing; many of threats are well-resourced, highly motivated, and sophisticated.[1]

Unlike most other federal agencies, however, NASA supports space-based science assets, the development of advanced technologies and systems, and on-orbit spaceflight operations that support the health and safety of NASA astronauts. Through these activities—and with their associated data and information—NASA is able to lead the world in space and Earth science discoveries, aeronautics research, space technology development, and human spaceflight and exploration. As space becomes a domain of increasing economic, societal, and geopolitical activity, advances in space technologies and capabilities can be important for securing value and influence for the Nation.

To accomplish its work, NASA manages an information technology (IT) portfolio that comprises both business IT, including institutional infrastructure to support broad agency operations, and mission IT, including the systems that operate spacecraft and collect or process scientific or technical data to support the agency's missions across space, science, and aeronautics. NASA's IT needs have led to the creation of a complex infrastructure with over 500 information systems and approximately 3,200 publicly accessible websites and web applications.[2] Information security and cybersecurity controls are a critical factor in protecting the confidentiality, integrity, and availability of IT systems and associated, highly valuable personal, scientific, proprietary, export-controlled, operational, and technical information at NASA.

Independent assessments of NASA's cybersecurity risk have reported that the agency's "vast connectivity with educational institutions, research facilities, and other outside organizations offers cybercriminals a larger target than most other government agencies and presents unique IT security challenges."[3] These assessments also found that NASA and its partners are consistently targeted by cybercriminals, some of whom could be sponsored by foreign intelligence services.[4]

More broadly, space operations—encompassing both in-space activities and associated ground systems—are seeing heightened risk of cyberattack, as capabilities advance and societal

[1] Since 1997, in recognition of this threat, the Government Accountability Office (GAO) has designated information security as a government-wide high-risk area in its biennial report to Congress. This was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. In a July 2019 report on this information security high-risk area, the GAO reported that "the risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated." In particular, the GAO reported increased sophistication of foreign adversaries' capabilities and the complicating factors of developments in artificial intelligence and Internet of Things technologies. Federal law, executive orders, and agency guidance provide instruction and resources for federal agencies to manage cybersecurity risks. The GAO report, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges," is available at: https://www.gao.gov/products/GAO-19-384.

[2] NASA Office of Inspector General, "2019 Report on NASA's Top Management and Performance Challenges," November 13, 2019. Available at: https://oig.nasa.gov/docs/MC-2019.pdf.

[3] *Ibid.*

[4] Government Accountability Office, "Urgent Action Needed to Address Significant Management and Cybersecurity Weakness," GAO-18-337, May 2018. Available at: https://www.gao.gov/assets/700/691916.pdf.

dependence on space infrastructure increases.[5] The White House recently issued a space policy directive that is intended to directly address some cybersecurity concerns for civil, commercial, and national security space infrastructure.[6]

Cybersecurity and Telework Under COVID-19

On March 15, 2020, the Office of Management and Budget (OMB) issued a memo directing federal agencies to maximize the use of telework flexibilities as part of the Nation's response to public health guidelines aimed at slowing the growing spread of the novel coronavirus, SARS-CoV-2.[7] Two days later, OMB directed federal departments and agencies to "immediately adjust operations and services to minimize face-to-face interactions," including by "maximizing telework across the nation for the Federal workforce (including mandatory telework, if necessary), while maintaining mission-critical workforce needs."[8] As local and regional public health directives imposed restrictions and NASA identified cases of COVID-19 among its workforce, individual NASA Centers were moved to mandatory telework status. By March 17, the agency had instituted mandatory telework for all but mission-essential staff at all NASA facilities.[9] As of September 16th, 2020 mandatory telework is still in effect at all NASA Centers and facilities, though some on-site mission-critical activities have been authorized to resume.[10]

As much of the federal workforce shifted to telework, the National Institute for Standards and Technology (NIST)[11] and the Department of Homeland Security (DHS) [12] published a number of resources offering guidance and best practices for both network administrators and employees during increases in telework, often applicable not only to federal workers, but also to the general public. For example, the National Cybersecurity Center of Excellence (NCCOE) at NIST,

[5] Harrison, Todd, Johnson, Kaitlyn, Roberts, Thomas G., Way, Tyler, and Young, Makena, "Space Threat Assessment 2020," Center for Strategic and International Studies Aerospace Security Project, March 2020. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V.

[6] President Donald Trump, "Cybersecurity Principles for Space Systems," *Memorandum on Space Policy Directive – 5*, September 4, 2020. Available at: https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

[7] Office of Management and Budget Memorandum M-20-15, March 15, 2020. Available at: https://www.whitehouse.gov/wp-content/uploads/2020/03/M20-15-Telework-Guidance-OMB.pdf.

[8] Office of Management and Budget Memorandum M-20-16, March 17, 2020. Available at: https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf.

[9] NASA Administrator Jim Bridenstine, "Statement on Agency Response to Coronavirus," Release 20-028, March 17, 2020. Available at: https://www.nasa.gov/press-release/nasa-administrator-march-17-statement-on-agency-response-to-coronavirus.

[10] https://nasapeople.nasa.gov/coronavirus/

[11] NIST develops standards and guidelines for all federal information systems and processes. The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The NIST National Initiative for Cybersecurity Education (NICE) establishes procedures that agencies are required to follow in hiring and management of their cybersecurity workforce. NIST Special Publication 800-171 provides requirements for government contractors to demonstrate they are adequately securing sensitive information and government systems.

[12] The DHS Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead for the Federal government's cybersecurity and has the authority to coordinate cybersecurity efforts across all Executive agencies. In support of Federal agencies, CISA provides security capabilities, including the National Cybersecurity Protection System (also known as EINSTEIN) and the Continuous Diagnostic and Mitigation (CDM) Program.

through the “Cybersecurity Insights” NIST blog, posted general guidance on telework security basics[13] and security for tele- and video-conferences.[14] CISA compiled a comprehensive list of do’s and don’ts of teleworking best practices.[15] CISA also provided guidance on using video conferencing software, highlighting the need to balance risk exposure from potential cybersecurity vulnerabilities related to the use of each video conferencing software with the benefits they provide to employees teleworking.[16] In addition, CISA published interim telework guidance to their Trusted Internet Connections (TIC) program, to provide security capabilities for remote federal employees securely connecting to agency networks and cloud environments.[17]

In April 2020, the Congressional Research Service (CRS) issued a report, “Federal Teleworking During the COVID-19 Pandemic: Cybersecurity Issues in Brief,”[18] which reported that increased telework was putting stress on federal communications infrastructure, data, and security. For example, the use of a virtual private network (VPN) client—which creates an encrypted tunnel allowing users to securely connect to an organization’s network with an external device—increased by 53% from early to mid-March as agencies began rapidly transitioning to telework. CRS also found that agencies’ use of virtual meeting software increased cybersecurity concerns due to unknown or inadequate privacy controls and encryption protocols of the commercial videoconferencing platforms. The CRS noted that the quick shift to substantial telework left little time for systems administrators to prepare their networks with improved policies and software updates. Further, since employees are no longer inside agency facilities, they lose the physical security of on-site work, and potential vulnerabilities in their home networks could present opportunities for access by bad actors.

Malicious actors also have a history of attempting to use high-profile events, especially by using people’s desire for new information to entice them to click on unsecure links or websites. In April 2020, after approximately one month of telework, the NASA Chief Information Officer (CIO) published an Agencywide memo alerting employees to an observed increase in cyber-attacks including increased phishing attempts, increased malware attacks on NASA systems, and increased instances of NASA systems trying to access malicious sites.[19]

[13] Greene, Jeff, "Telework Security Basics," *Cybersecurity Insights: A NIST blog*, March 19. Available at: https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics.
[14] Greene, Jeff, "Preventing Eavesdropping and Protecting Privacy on Virtual Meetings," *Cybersecurity Insights: A NIST blog*, March 17, 2020. Available at: https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings.
[15] *Ibid.*
[16] Cybersecurity and Infrastructure Agency, “Video Conferencing Guide.” Available at: https://www.cisa.gov/video-conferencing-guidance.
[17] Federal Mobility Group, “Cybersecurity Experts Provide Remote Work Best Practices,” *Cio.gov*, July 8, 2020. Available at: https://www.cio.gov/cybersecurity-experts-provide-remote-work-best-practices/.
[18] Jaikaran, Chris, “Federal Telework During the COVID-19 Pandemic: Cybersecurity Issues in Brief,” *Congressional Research Service*, April 10, 2020. Available at: https://crsreports.congress.gov/product/pdf/R/R46310.
[19] NASA CIO, “Cyber Threats Significantly Increasing During Coronavirus Pandemic,” *Spaceref.com*, April 6, 2020. Available at: http://spaceref.com/news/viewsr.html?pid=53512.

Information Technology and Cybersecurity Management Structure at NASA

NASA spent approximately $2.3 billion on computer systems, networks, and other information technology (IT) in fiscal year (FY) 2019 in support of the activities of the more than 17,000 civil servants and 40,000 contractors across nine Centers and one Federal Funded Research and Development Center around the country. The agency CIO reports directly to the NASA Administrator and leads the headquarters-based Office of the Chief Information Officer (OCIO), which is responsible for the planning, policy, and oversight for the management of NASA's data and information technology.[20] The OCIO also ensures the Agency's IT assets are acquired and managed in a manner consistent with federal policies and statutory requirements, including the Federal Information Security and Modernization Act (FISMA).[21]

In FY2020, the OCIO has more than 175 employees organized into five divisions: Applications, Cybersecurity and Privacy, Enterprise Services and Integration, IT Business Management, and Transformation Data.[22] In addition to the Agency CIO, each of the nine NASA centers has a CIO and each Mission Directorate has an IT official with the duties of a CIO.[23] The CIO relies on Center CIOs and staff to implement and enforce the Agency's information security policies.

NASA's CIO appoints a Senior Agency Information Security Officer (SAISO), who is responsible for NASA's information and cybersecurity program. The NASA SAISO, through the Cybersecurity and Privacy Division, manages the Agency-wide information and cybersecurity program to correct known vulnerabilities, reduce barriers to cross-Center collaboration and provide cost effective cybersecurity services in support of NASA's information systems.[24] In FY2019, NASA reported spending $167.6 million on cybersecurity, a $3.1 million decrease (1.8%) from FY2018, but a $33.2 million (24.7%) increase over the average reported spending for the last five fiscal years.[25]

NASA's information security program is managed through the Risk Information Compliance System (RISCS), a data repository that identifies and maintains an inventory of the agency's hardware and software, including a system security plan (SSP) and a contingency plan for each information system. RISCS also maintains the Agency Common Control (ACC) system, which

[20] NASA Information Technology Strategic Plan (Fiscal Years 2018-2021) Available at: https://www.nasa.gov/sites/default/files/atoms/files/itsp_10sept19_508.pdf_0.pdf.

[21] The *Federal Information Security Modernization Act of 2014* (FISMA, P.L. 113-283) requires federal agencies to develop, document, and implement an agency-wide information security program for information security systems supported or managed by the agency commensurate with their risk profile.

[22] NASA Office of Inspector General, "Evaluation of NASA's Information Security Program Under the Federal Information Security Modernization Act for FY 2019," IG-20-017, June 25, 2020. Available at: https://oig.nasa.gov/docs/IG-20-017.pdf.

[23] NASA Office of Inspector General, "Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices," IG-20-021, August 27, 2020 Available at: https://oig.nasa.gov/docs/IG-20-021.pdf.

[24] NASA Office of the CIO, "Cybersecurity and Privacy Division." Available at: https://www.nasa.gov/offices/ocio/cybersecurity-privacy.

[25] Office of Management and Budget, "Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2019," Available at: https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf.

aggregates and manages all Agency-level common controls (controls that support multiple information systems) as a single system security plan.

NASA is currently attempting to improve its cybersecurity and IT management with multiple Agency-wide initiatives. The OCIO is leading the NASA Strategy to Improve Network Security (NSINS) to better secure NASA's networks, systems, and data by modernizing, simplifying, and securing the agency's IT systems and how employees gain access to those systems.[26] Longstanding efforts also continue within the OCIO to transition the agency to a more efficient enterprise operating model for IT and cybersecurity. The NASA CIO testified to Congress in December 2019 that one such effort, an activity under NASA's Mission Support Future Architecture Program (MAP), is to be implemented after undergoing assessment and planning that should conclude by December 2020.[27]

Assessments of NASA Information Security and Cybersecurity Management

In its most recent report on NASA's top management and performance challenges, the Office of Inspector General (OIG) stated that, for more than twenty years, NASA's OCIO "has struggled to implement an effective IT governance structure that aligns authority and responsibility commensurate with the agency's overall mission." For more than 10 years, the OIG has included securing the agency's IT systems and data as a top challenge facing NASA. The OIG cites a specific concern that the "decentralized nature of NASA's operations and its long-standing culture of autonomy hinder the OCIO's ability to implement effective IT governance."[28] The OIG continues to find that the decentralized nature "has allowed Centers to tailor processes to meet their own priorities, which has led to inconsistency in NASA's strategic IT management."

The OIG has also regularly found NASA's IT management practices to fare poorly against federal requirements and assessments. The FY2019 Office of Management and Budget (OMB) FISMA report to Congress[29] in January 2020 indicated that most agencies within the federal government were demonstrating positive trends in modernizing IT infrastructure, adopting recommended cybersecurity approaches, and reducing or mitigating vulnerabilities, and the number of cybersecurity incidents were generally trending downward. However, NASA's FY2019 FISMA assessment showed an increase in the number of cybersecurity incidents,[30] and

[26] NASA Information Technology Strategic Plan (Fiscal Years 2018-2021) Available at: https://www.nasa.gov/sites/default/files/atoms/files/itsp_10sept19_508.pdf_0.pdf.

[27] Written Testimony of Renee Wynn, NASA Chief Information Officer, to the Government Operations Subcommittee of the House Committee on Government Oversight and Reform, December 11, 2019. Available at: https://docs.house.gov/meetings/GO/GO24/20191211/110318/HHRG-116-GO24-Wstate-WynnR-20191211.pdf

[28] NASA Office of Inspector General, "2019 Report on NASA's Top Management and Performance Challenges," November 13, 2019. Available at: https://oig.nasa.gov/docs/MC-2019.pdf.

[29] The OMB is responsible for overseeing Federal agencies' cybersecurity and for developing and directing implementation of new policies and guidelines. Under FISMA, agency CIOs and Inspectors General submit reports to OMB on their respective agencies' cybersecurity performance, which are then distilled into an annual report to Congress. The annual OMB reports include data on cybersecurity incidents and both self-assessments and independent assessments of agencies' information security programs. The FY2019 OMB FISMA report to Congress is available at: https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf.

[30] *Ibid*.

the OIG's independent assessment gave NASA's information security systems a Level 2 rating, or "Defined," (on a scale of 1-5, with 5 being "Optimized") for the fourth year in a row.[31]

The OIG's FY2019 FISMA assessment evaluated NASA's IT management and cybersecurity program against FISMA guidelines and concluded that NASA "has not implemented an effective Agency-wide information security program." [32] The OIG found numerous instances of inaccuracies, inconsistencies, and missing or out of date information in various system security plans, contingency plans, and other IT security handbooks and documents; that known deficiencies in information systems controls were not being addressed in plans; inconsistent requirement of RISCS as the agency's information security management tool; and insufficient awareness by NASA information security personnel of Agency information security policies and procedures. To address these concerns and strengthen NASA's information security program, the OIG issued nine recommendations to NASA, including such actions as ensuring the agency's information system oversight process is adequate, implementing a policy to enforce Agency-wide requirements, and making sure system security plans are updated in accordance with FISMA requirements.[33] NASA concurred with all nine recommendations and plans to implement them by November 2021.

The Government Accountability Office (GAO) has similarly raised concerns for many years about NASA's cybersecurity risk management and identified it as a top challenge for the agency. GAO reported in July 2019 that certain agencies, including NASA, had not fully addressed key practices that are foundational to effectively managing cybersecurity risks.[34] Two recommendations from that report remain open and were included in GAO's April 2020 update to its list of "priority" open recommendations for NASA.[35] In particular, the GAO highlighted its recommendation that NASA "establish a process for conducting an organization-wide cybersecurity risk assessment." NASA concurred with the recommendation and has stated that it would be met by the end of September 2020.

Several recent, more narrowly focused NASA OIG audits of various agency and partner systems and programs found cybersecurity vulnerabilities and implementation challenges associated with contractor-managed activities. A June 2019 audit of NASA's Jet Propulsion Laboratory (JPL), a federally-funded research and development center (FFRDC) managed by the California Institute of Technology under contract to NASA, found that "multiple IT security control weaknesses reduce JPL's ability to prevent, detect, and mitigate attacks targeting its systems and networks, thereby exposing NASA systems and data to exploitation by cyber criminals."[36] A March 2020 audit of NASA's management of its Earth Science Distributed Active Archive Centers revealed

[31] NASA Office of Inspector General, "Evaluation of NASA's Information Security Program Under the Federal Information Security Modernization Act for Fiscal Year 2019," IG-20-017, June 25, 2020. Available at: https://oig.nasa.gov/docs/IG-20-017.pdf.

[32] *Ibid.*

[33] *Ibid.*

[34] Government Accountability Office, "Agencies Need to Fully Establish Risk Management Programs and Address Challenges," GAO-19-384, July 2019. Available at: https://www.gao.gov/assets/710/700503.pdf.

[35] Government Accountability Office, "Priority Open Recommendations: National Aeronautics and Atmospheric Administration," GAO-20-526PR, April 30, 2020. Available at: https://www.gao.gov/products/GAO-20-526PR.

[36] NASA Office of Inspector General, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory," IG-19-022, June 18, 2019. Available at: https://oig.nasa.gov/docs/IG-19-022.pdf.

deviations from NIST and NASA cybersecurity guidance and policies due to "a lack of close OCIO involvement," and recommended NASA consider updating its policies to ensure involvement of and coordination with OCIO early in mission development.[37] Also in March 2020, the OIG reported that NASA's Exploration Ground Systems (EGS) and Orion programs experienced unexpected challenges in establishing necessary remote access for an EGS major software development team (comprised of both NASA and Jacobs workers) to an Orion testbed managed by Lockheed Martin for NASA. The OIG found that challenges meeting and resolving IT and cybersecurity requirements from both NASA and Lockheed Martin in order to grant the software team remote access to the testbed contributed to a two-year delay in the software development program.[38]

In August 2020, the NASA OIG issued the results of an audit of NASA's policies and practices regarding non-agency IT devices, such as personal cell phones, tablets, or laptops.[39] NASA allows personally-owned devices of NASA employees and NASA partner employees to securely connect to some of NASA's internal networks and systems, if certain requirements are met and software management is installed on the device. In the report, the OIG found that NASA is "not adequately securing its networks from unauthorized access by IT devices." The OIG further found that the NASA CIO is not monitoring and enforcing rules for granting access to NASA's networks for personal devices and has limited visibilities into IT authorization practices at the Centers and other NASA-managed facilities. The OIG warned that these shortcomings increase NASA's vulnerability to improper use and unauthorized access to NASA's internal networks. NASA concurred with the report's five recommendations, which NASA estimates will be addressed by December 2021. In March 2020, the NASA OIG initiated an audit of NASA's overall cybersecurity readiness, which remains ongoing at the time of this hearing.

[37] NASA Office of Inspector General, "NASA's Management of Distributed Active Archive Centers," IG-20-011, March 3, 2020. Available at: https://oig.nasa.gov/docs/IG-20-011.pdf.

[38] NASA Office of Inspector General, "NASA's Development of Ground and Flight Software for the Artemis Program," IG-20-014, March 19, 2020. Available at: https://oig.nasa.gov/docs/IG-20-014.pdf.

[39] NASA Office of Inspector General, "Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices," IG-20-021, August 27, 2020. Available at: https://oig.nasa.gov/docs/IG-20-021.pdf.