CYBERSECURITY AT NASA: ONGOING CHALLENGES AND EMERGING ISSUES FOR INCREASED TELEWORK DURING COVID–19

HEARING

BEFORE THE

SUBCOMMITTEE ON SPACE AND AERONAUTICS

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 18, 2020

Serial No. 116–81

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
41–348PDF WASHINGTON : 2021

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California,
Vice Chair
LIZZIE FLETCHER, Texas
HALEY STEVENS, Michigan
KENDRA HORN, Oklahoma
MIKIE SHERRILL, New Jersey
BRAD SHERMAN, California
STEVE COHEN, Tennessee
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
BEN MCADAMS, Utah
JENNIFER WEXTON, Virginia
CONOR LAMB, Pennsylvania

FRANK D. LUCAS, Oklahoma,
Ranking Member
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANDY BIGGS, Arizona
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
MICHAEL CLOUD, Texas
TROY BALDERSON, Ohio
PETE OLSON, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JIM BAIRD, Indiana
FRANCIS ROONEY, Florida
GREGORY F. MURPHY, North Carolina
MIKE GARCIA, California
THOMAS P. TIFFANY, Wisconsin

SUBCOMMITTEE ON SPACE AND AERONAUTICS

HON. KENDRA HORN, Oklahoma, *Chairwoman*

ZOE LOFGREN, California
AMI BERA, California
ED PERLMUTTER, Colorado
DON BEYER, Virginia
CHARLIE CRIST, Florida
JENNIFER WEXTON, Virginia

BRIAN BABIN, Texas, *Ranking Member*
MO BROOKS, Alabama
BILL POSEY, Florida
MICHAEL WALTZ, Florida
MIKE GARCIA, California

C O N T E N T S

September 18, 2020

CYBERSECURITY AT NASA: ONGOING CHALLENGES AND EMERGING ISSUES FOR INCREASED TELEWORK DURING COVID–19

FRIDAY, SEPTEMBER 18, 2020

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON SPACE AND AERONAUTICS,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 11:01 a.m., via Webex, Hon. Kendra Horn [Chairwoman of the Subcommittee] presiding.

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.

Chairwoman HORN. Good morning, everyone. I'd like to welcome our distinguished panel of witnesses, Members, and those viewing remotely, to today's Space and Aeronautics Subcommittee hearing on "Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID–19".

In early 2020 the world was caught off guard with the rapid and dramatic onset of the coronavirus. NASA (National Aeronautics and Space Administration), like many Federal agencies, and consistent with the Office of Management and Budget (OMB) Guidance, rapidly shifted to telework operations to ensure the health and safety of its more than 17,000 civil servant employees and extensive contractor workforce. To its credit, NASA prepared for the transition, having held an agency-wide telework exercise in early March to test expanded telework operations, and today 75 to 80 percent of NASA civil servants continue to work remotely, handling proposal reviews, project oversight and inspections, development work, engineering analysis, and other activities.

The shift to increased telework at NASA raises many questions, front and center, cybersecurity. What does the increase and extended use of telework mean for protecting NASA's intellectual property, personally identifiable information (PII), and mission operations? How do the cyber challenges related to increased telework affect the agency's overall cybersecurity risk posture, and what steps is NASA taking to ensure the effectiveness of its cybersecurity efforts during the pandemic and beyond? These are some of the questions today's hearing will explore, because what's clear is that NASA is a target. And I want to pause here for a moment to note an article in *The Hill* today where the Justice Department has brought charges against Iranian nationals for hacking U.S. satellite companies, so I think this is incredibly timely. And a recent NASA IG (Inspector General) report stated that, given NASA's mission, and valuable technical and intellectual capital it produces, the information maintained within the agency's IT (information technology) infrastructure presents a high value target for hackers and criminals.

In 2019 NASA Administrator Jim Bridenstine stated at an agency town hall that NASA is the most attacked agency in the Federal Government when it comes to cybersecurity. Past data breaches and system intrusions at NASA and its facilities have resulted in large amounts of stolen data, installation of malware, copying, modifying, and deleting sensitive files, and accessing NASA servers, including those supporting missions. The Department of Homeland Security's (DHS's) Cybersecurity Infrastructure Security Agency, which is a mouthful, of course—but a very important agency has issued specific alerts on vulnerabilities related to telework during the pandemic, and encourages organizations to adopt a heightened state of cybersecurity.

In April 2020 the agency's then Chief Information Officer (CIO) notified employees of increased hacking attempts on the agency's systems, and in June 2020 media articles reported that malicious actors congratulated NASA and SpaceX on a crewed demonstration flight, and then announced they had allegedly breached and infected a NASA contractor, specifically one that provides information technology cyber securities—and cybersecurity services to the

agency. If true, that's a concerning report, and part of the reason we're here today. Protecting NASA's IT and data during the pandemic demands vigilance, however, NASA's cybersecurity challenges don't begin and end with the COVID–19 crisis. Multiple NASA IG and GAO (Government Accountability Office) reports have identified weaknesses and ongoing concerns with NASA's information security. Further, they've ranked this issue as a top agency challenge. Ensuring effective cybersecurity at NASA becomes even more pressing given rapid advances in IT supply chain risks, NASA's culture of openness and partnerships, and the overall increase in space activities.

NASA is a national treasure. Its missions continue to inspire both young and old, and NASA's cutting edge space technologies, research, and space flight experience are the envy of the world. NASA's accomplishments wouldn't be possible without computers, software, and information systems. Will NASA, or any organization, ever be 100 percent risk free from cyber threats? Probably not. Is there room for improvement? Absolutely there is. I hope that today's hearing will give an understanding of the challenges and risks posed by increased telework, and whether or not NASA is organized and resourced sufficiently and effectively to mitigate those risks. The bottom line is we need to ensure that NASA has the tools that it needs, and takes the necessary actions to ensure the agency's success, safety, and security during COVID–19 and beyond, and I look forward to our witnesses' testimony today.

[The prepared statement of Chairwoman Horn follows:]

Good morning. I'd like to welcome our distinguished panel of witnesses, Members, and those viewing remotely, to today's Space and Aeronautics Subcommittee hearing on "Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19".

In early 2020, the world was caught off guard with the rapid and dramatic onset of the coronavirus. NASA, like many Federal agencies, and consistent with Office of Management and Budget guidance, rapidly shifted to telework operations to ensure the health and safety of its more than 17,000 civil servant employees and extensive contractor workforce.

To its credit, NASA prepared for the transition, having held an agency-wide telework exercise in early March to test expanded telework operations. Today, 75 to 80 percent of NASA civil servants continue to work remotely handling proposal reviews, project oversight and inspections, development work, engineering analysis, and other activities.

The shift to increased telework at NASA raises many questions. Front and center is cybersecurity.

• What does the increase and extended use of telework mean for protecting NASA' intellectual property, personally identifiable information, and mission operations?

• How do the cyber challenges related to increased telework affect the agency's overall cybersecurity risk posture?

• And what steps is NASA taking to ensure the effectiveness of its cybersecurity efforts during the pandemic and beyond?

These are some of the questions today's hearing will explore, because what's clear is that NASA is a target.

A recent NASA IG report stated, "Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals."

In early 2019, NASA Administrator Jim Bridenstine stated at an agency town hall that "NASA is one of the—it is the most attacked agency in the Federal government when it comes to cybersecurity." Past data breaches and system intrusions at NASA and its facilities have resulted in large amounts of stolen data; installation of malware; copying, modifying, and deleting sensitive files; and accessing NASA servers, including those supporting missions.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency—CISA—has issued specific alerts on vulnerabilities related to telework

during the pandemic and encourages organizations "to adopt a heightened state of cybersecurity."

In April 2020, the agency's then-chief information officer notified employees of increased hacking attempts on the agency's systems. And in June 2020, media articles reported that malicious actors congratulated NASA and SpaceX on a crewed demonstration flight, and then announced they had allegedly breached and infected a NASA contractor, specifically one that provides information technology and cybersecurity services to the agency. If true, that's a concerning report, and part of the reason we're here today.

Protecting NASA's IT and data during the pandemic demands vigilance. However, NASA's cybersecurity challenges don't begin and end with the COVID crisis. Multiple NASA IG and GAO reports have identified weaknesses and ongoing concerns with NASA's information security; further, they have ranked the issue as a top agency challenge.

Ensuring effective cybersecurity at NASA becomes even more pressing, given rapid advances in IT, supply chain risks, NASA's culture of openness and partnerships, and the overall increase in space activities.

NASA is a national treasure. Its missions continue to inspire both young and old and NASA's cutting-edge space technologies, research, and spaceflight experience are the envy of the world. NASA's accomplishments wouldn't be possible without computers, software, and information systems.

Will NASA or any organization ever be 100 percent risk-free from cyber threats? Probably not. Is there room for improvement? Most definitely, yes.

I hope today's hearing will give us an understanding of the challenges and risks posed by increased telework, and whether or not NASA is organized and resourced to effectively mitigate those risks. Bottom line: we need to ensure that NASA has the tools and takes the necessary actions to ensure the agency's success, safety, and security, during COVID, and beyond.

I look forward to our witnesses' testimony.

Chairwoman HORN. So I think we are—there he is——

Mr. BABIN. Hey, Chairman.

Chairwoman HORN. Ranking Member Babin, I'm glad you were able—I know that technology can sometimes, speaking of technology, be a little bit of a challenge, but glad you made it through. So the Chair now recognizes Ranking Member Babin, and my good friend from Texas, for an opening statement.

Mr. BABIN. Absolutely, thank you. We have three computers here. We couldn't get on, but I got on with my telephone, any way we can do it, I'm glad to be with you.

Chairwoman HORN. And—innovation and ingenuity, I love it.

Mr. BABIN. Absolutely. OK. Well, thank you so much. NASA is one of the best-known organizations in the entire world. Its successes with the Mercury, Gemini, Apollo, Shuttle, and International Space Station programs, along with its breathtaking scientific discoveries and jaw-dropping robotic probes attract worldwide attention. Unfortunately, that attention comes with many challenges. The technologies that NASA develops are also sought after by criminal entities, unscrupulous foreign governments, and destructive vandals. Because many of these technologies have both civil and military applications, these challenges are particularly great, and this is a topic that this Committee has focused on for decades.

Mr. Martin testified before the Investigations and Oversight Subcommittee almost 10 years ago on the topic of information security. At that hearing he testified that an unencrypted laptop was stolen from NASA that resulted in the loss of the "algorithms" used to control the Space Station, as well as personally identifiable information, and intellectual property. Similarly, the U.S.-China Economic and Security Review Commission noted, in its 2011 report

to Congress, that the Terra and Landsat 7 satellites experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems.

More recently the NASA IG issued its yearly *FISMA* (*Federal Information Security Management Act*) report in July, which found that "Information systems throughout the agency face an unnecessarily high level of risk that threatens the confidentiality, the integrity, and availability of NASA's information." The report concluded that, "It is imperative the agency continue its efforts to strengthen its risk management and governance practices to safeguard its data from cybersecurity threats." And last month the IG issued another report on NASA's use of non-agency IT devices and found that NASA, "is not adequately securing its networks from unauthorized access by IT devices." The NASA IG is currently tracking 25 open recommendations for the Office of the Chief Information Officer. These do not include IT and cybersecurity recommendations to mission directorates or other organizations in the NASA enterprise.

And while this may seem startling, there are specific reasons that many of the recommendations remain open. For instance, agency-wide guidelines and best practices are often general rules and principles that are not optimized to specific agencies unique capabilities, expertise, and challenges. For instance, NASA is the world leader in designing, building, operating, and communicating with spacecraft. This expertise resides within the mission directorates, and at the centers who have cultivated this expertise over many decades. In some instances they actually developed the software, information systems, and underlying technologies that industry and the rest of the government adopted and embraced. In even more extreme circumstances, they continue to use one-off operating systems that, while perhaps not compliant with OMB derived governmentwide guidance, are arguably more secure because of their uniqueness and their obscurity. Efforts to bring these systems and technologies into compliance with a one-size-fits-all cookie cutter approach developed for commercial enterprise systems could actually introduce more risk into the system. This isn't to excuse NASA's cybersecurity shortcomings, as identified by the IG and GAO over the years. Lost laptops, unsecured devices, unauthorized access to systems, and lapsed ATOs, or authorization to operate, and poor inventory management are all cause for concern. Which brings us to the situation that NASA currently faces.

The COVID–19 challenge requires most of NASA's employees and contractors to work remotely. And while NASA has embraced teleworking for years, the expansion of this practice introduces a larger target and more vulnerabilities for malicious actors to exploit. In addition to teleworking challenges, I'm also interested in understanding what level of insight that NASA has on contractor cybersecurity as NASA moves more to public-private partnerships. And finally, it's worth noting that President Trump recently issued Space Policy Directive Number Five, focused on cybersecurity principles for space systems. And while it is not COVID-focused specifically, it is particularly timely, given today's hearing and demonstration of the administration's forward-looking leadership on this very topic.

I look forward to hearing more about these important issues, and what NASA plans to do to mitigate them, as well as what Congress and the administration can do to help. So, with that, Madam Chair, I yield back.

[The prepared statement of Mr. Babin follows:]

NASA is one of the best-known organizations in the world. Its successes with the Mercury, Gemini, Apollo, Shuttle, and International Space Station programs—along with its breathtaking scientific discoveries and jaw-dropping robotic probes—attract worldwide attention. Unfortunately, that attention comes with challenges. The technologies that NASA develops are also sought-after by criminal entities, unscrupulous foreign governments, and destructive vandals. Because many of these technologies have both civil and military applications, these challenges are particularly grave.

This is a topic that this Committee has focused on for decades. One of our witnesses, NASA Inspector General Martin, testified before the Investigations and Oversight Subcommittee almost ten years ago on information security. At that hearing, he testified that an unencrypted laptop was stolen from NASA that "resulted in the loss of the algorithms" used to control the space station, as well as personally identifiable information and intellectual property.

Similarly, the U.S. China Economic and Security Review Commission noted in its 2011 report to Congress that the Terra and Landsat-7 satellites "experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems." More recently, the NASA Office of the Inspector General issued its yearly *FISMA* report in July, which found that ". . . information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA's information." The report concluded that ". . . it is imperative the Agency continue its efforts to strengthen its risk management and governance practices to safeguard its data from cybersecurity threats." And last month, the NASA Office of the Inspector General issued another report on NASA's use of non-agency IT Devices that found that "NASA is not adequately securing its networks from unauthorized access by IT devices." The NASA Inspector General is currently tracking 25 open recommendations for the Office of the Chief Information Officer. These do not include IT and cybersecurity recommendations to Mission Directorates or other organizations in the NASA enterprise.

While this may seem startling, there are specific reasons that many of the recommendations remain open. For instance, agency-wide guidelines and best practices are often general rules and principles that are not optimized to specific agencies unique capabilities, expertise, and challenges. For example, NASA is the world leader in designing, building, operating, and communicating with spacecraft. This expertise resides within the Mission Directorates and at the Centers who have cultivated this skillset over decades. In some instances, they actually developed the software, information systems, and underlying technologies that industry and the rest of the government adopted and embraced.

In even more extreme circumstances, they continue to use one-off operating systems that, while perhaps not compliant with OMB-derived government-wide guidance, are arguably more secure because of their uniqueness and obscurity. Efforts to bring these systems and technologies into compliance with one-size-fits-all, cookie-cutter approaches developed for commercial and enterprise systems could actually introduce more risk. This isn't to excuse NASA's cybersecurity shortcomings as identified by the IG and GAO over the years. Lost laptops, unsecured devices, unauthorized access tosystems, and lapsed ATOs (or "Authorization to Operate"), and poor inventory management are all cause for concern.

Which brings us to the situation NASA currently faces. The COVID-19 challenge requires most of NASA's employees and contractors to work remotely. While NASA has embraced teleworking for years, the expansion of this practice introduces a larger target and more vulnerabilities for malicious actors to exploit.

In addition to teleworking challenges, I am also interested in understanding what level of insight NASA has on contractor cybersecurity as NASA moves more to public-private partnerships. Finally, it's worth noting that President Trump recently issued Space Policy Directive 5 focused on cybersecurity principles for space systems. While it is not focused on COVID specifically, it is particularly timely given today's hearing and demonstrates the Administration's forward-looking leadership on the topic.

I look forward to hearing more about these critical issues, what NASA plans to do to mitigate them, as well as what Congress and the Administration can do to help.

Thank you, I yield back.

Chairwoman HORN. Thank you, Ranking Member Babin, for your opening statement. I think it's safe to say we share many of the same concerns in this area, and I'm excited and grateful for the opportunity for this hearing today. If there are any Members who wish to—at this point, if there are any Members who wish to submit additional opening statements, your statements will be added to the record at this point.

[The prepared statement of Chairwoman Johnson follows:]

Good morning Chairwoman Horn, Ranking Member Babin, and Members of the Subcommittee. To our witnesses, welcome and thank you for being here.

As we ushered in 2020 and a new decade, none of us could have predicted that we'd be here today, six months into a new way of living and working in order to protect our own and others' health from COVID-19.

Thanks to the internet, information technology, and communication services, many Americans can continue to interact with family and friends-albeit virtually-and work remotely. That includes NASA's workforce.

To its credit, NASA is accomplishing a lot in this virtual, telework environment, though some mission-essential employees are still working on-site.

• NASA and its partner, SpaceX, successfully carried out a commercial crew demonstration mission to the International Space Station;

• the Orion program completed key reviews to certify that the crew vehicle is ready for flight;

• engineers are operating some science spacecraft from their homes; and

• the OSIRIS-REx team successfully completed a final dress rehearsal in advance of collecting samples from asteroid Bennu next month.

I'm pleased that NASA's can-do spirit is prevailing, despite the challenges of this pandemic. But with so many important NASA operations being carried out away from the institutional security of NASA facilities, I'm concerned about cybersecurity.

Space is hard and risky, and NASA has exceptional skills at managing risk. When it comes to cybersecurity and information technology management, however, NASA struggles.

The agency continues to lack a cybersecurity risk management strategy, as recommended by GAO, and both GAO and the NASA Inspector General have cited information security as a top challenge for NASA.

Unfortunately, NASA's lagging performance on cybersecurity isn't new, it's a continuing problem. For many years, NASA IG and GAO reports have identified deficiencies and management challenges in NASA's information security.

And now, with COVID, NASA-like other organizations-must protect against cyber criminals and malicious actors who are increasing their efforts to access government, business, and personal data and IT systems while employees work from home.

I have no doubt that NASA officials are working hard to keep the agency's IT systems and data safe, and I understand they are making some progress.

However, long-standing, recommended actions to improve NASA's cybersecurity have been left undone. In addition, the agency's approach to IT security is fragmented and the Chief Information Officer continues to lack the ability to manage NASA's cybersecurity efforts across the agency. NASA can and must to better.

In closing, NASA is a catalyst for inspiration, an engine of discovery and innovation, and a world leader in the peaceful uses and exploration of outer space.

We can't afford to let bad actors and cyber criminals threaten the safety and success of NASA's science, aeronautics research, space technology, and human spaceflight programs.

I look forward to hearing from our witnesses on what is needed to ensure that robust and effective cybersecurity protections are in place at NASA now, during COVID-19, and into the future.

Thank you, and I yield back.

Chairwoman HORN. And now I'd like to introduce our witnesses. Our first witness today is Mr. Jeff Seaton. In April 2020 Mr. Seaton was named NASA's Chief—Acting Chief Information Officer—Acting Chief Information Officer, let's see if I can get that out right. Prior to his current position, Mr. Seaton served as NASA's Deputy Chief Information Officer, and spent 7 years as the Chief Information Officer at NASA's Langley Research Center. He began his career with NASA in 1991 as a research engineer, designing robotic systems for space-based applications, and also served as Langley's Chief Technology Officer and Deputy CIO. Mr. Seaton received a Bachelor's Degree and Master's Degree in Electrical Engineering from Virginia Tech. Welcome, Mr. Seaton. We're glad you're with us today.

Our next witness is Mr. Paul Martin, Inspector General for the National Aeronautics and Space Administration. Mr. Martin has been the NASA Inspector General since 2009, and prior to his appointment at NASA, he served as the Deputy Inspector General at the Department of Justice. He also spent 13 years at the U.S. Sentencing Commission, including 6 years as the commission's deputy staff director. Mr. Martin received a Bachelor's Degree in Journalism from Pennsylvania State University, and a Juris Doctorate from Georgetown University Law Center. Welcome, Mr. Martin.

Our third and final witness today is Dr. Diana Burley. In July 2020 Dr. Burley was appointed as Vice Provost for Research and Professor of Public Administration at American University. Prior to her current position, Dr. Burley spent 13 years as a professor of human and organizational learning at George Washington University, where she was the inaugural Chair for the Human and Organizational Learning Department, and the Director of Executive Leadership doctoral program. She has also managed a multi-million-dollar computer science education and resource portfolio for the National Science Foundation. Dr. Burley received a Bachelor's Degree in Economics from The Catholic University of America, a Master's in Public Management and Policy from Carnegie Mellon University, and Master's and Doctoral Degrees in Organizational Science and Information Policy, also from Carnegie Mellon University. Welcome, Dr. Burley.

As our witnesses, you should you know you each have 5 minutes for your spoken testimony. Your written testimony will be included in the record for this hearing. When you have completed your spoken testimony, we will begin with questions, and each Member will have 5 minutes to question the panel. We'll start today with Mr. Seaton. Mr. Seaton, you're recognized for 5 minutes.

TESTIMONY OF MR. JEFF SEATON, CHIEF INFORMATION OFFICER (ACTING), NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Mr. SEATON. Thank you, Chairwoman Horn, Ranking Member Babin, and Members of the Subcommittee on Space and Aeronautics, for allowing me to appear before you today and talk about

NASA's information technology infrastructure, and our efforts to manage and protect that infrastructure during the COVID–19 pandemic. Thankfully, due to strategic investments made over the last several years, NASA was well positioned to keep our missions moving forward by shifting the majority of our workforce to telework last March. As a result, NASA has never been closed, and our workforce has continued to work remotely in a productive, and often creative, manner, despite the highly contagious COVID–19 virus. With strict safety protocols in place, NASA is now gradually allowing more employees onsite, based on factors such as local conditions, and guidance from the CDC (Centers for Disease Control) and other Federal partners. Let me assure you, the safety of our workforce remains our top priority. At the same time, protecting and effectively operating our IT infrastructure continues to be another top, massive focus.

IT plays a critical role of every aspect of NASA's missions. However, effective IT management is not an easy task. As NASA's Acting Chief Information Officer, it's my job to balance implementing innovative, mission-enabling IT capabilities with operational efficiency and effective cybersecurity to guard against evolving threats. During the pandemic the demands and expectations placed on NASA's IT infrastructure have been incredibly high, and the threats from external actors remain an ongoing concern. However, with hard work, dedication, and innovation, NASA's CIO team has risen to the challenge of keeping our missions moving forward. For example, OCIO (Office of the Chief Information Officer) helped rapidly develop software to track cases of onsite COVID–19 exposures, while also meeting all security and privacy requirements. Additionally, with OCIO's help, NASA continues to hire and onboard new employees, contractors, and interns with innovative approaches to provisioning and maintaining IT systems and tools remotely.

For NASA employees the pandemic has dramatically changed the way that we work. While many employees already teleworked at least occasionally before the pandemic, having 90 percent of employees teleworking at the same time has been game changing. NASA employees have significantly increased their use of virtual collaboration tools, such as Webex and Microsoft Teams, so we can interact with each other face to face while sharing virtual collaborative workspaces. Employees are dependent on NASA's virtual private network (VPN) to connect securely to internal networks and systems. Before the pandemic, our highest VPN connection rate was about 12,000 users in a single day. Today our VPN is supporting almost 40,000 daily users, with an availability exceeding 99 percent, thanks to architectural and capacity improvements implemented over the past 24 months.

Like other Federal agencies, NASA's IT infrastructure is under constant attack from well-resourced and highly motivated domestic and foreign adversaries, and we remain a popular target today. Therefore, we continue to strengthen our technical and procedural capabilities to proactively defend and protect our systems and data. While the reported number of attempted cyber incidents continues to increase partly because we have greater visibility into our network today, I'm confident that NASA is appropriately addressing and strengthening our response to these threats.

In Fiscal Year 2020 NASA developed a continuity of operations capability to further enhance our security operations center (SOC), located at the Ames Research Center. Previously, if SOC operations were disrupted, we had a limited ability to identify, detect, and respond to incidents. Today NASA SOC operations span multiple centers, allowing us to maintain 24 by 7 SOC operations at all times, even if there is an isolated disruption. With strengthened tools and capabilities, NASA is transitioning from a largely reactive to a more proactive cybersecurity posture. As the pandemic worsened in April, NASA even moved the SOC to remote operations to ensure employee safety, and we did so without negatively impacting our network or our cybersecurity capabilities.

In closing, I want to personally thank not only my OCIO staff and leadership, but the entire NASA workforce for their hard work, and the personal sacrifices they've made during this challenging time. Our employees are finding new ways to keep missions moving forward, support each other, balance work and family pressures, and even dedicate their expertise and personal time to developing technologies that are aiding in the national response to the coronavirus. While no one is sure what the future holds, NASA's senior leaders, including myself, are committed to keeping the NASA workforce safe, and providing them with the IT tools and infrastructure they need to continue executing our missions. I want to assure you that protecting and evolving NASA's IT infrastructure is, and will remain, a top agency priority. Thank you for the opportunity to testify before you today, and I look forward to answering any of your questions. Thank you.

[The prepared statement of Mr. Seaton follows:]

National Aeronautics and
Space Administration

Hold for Release Until
Presented by Witness

September 18, 2020

Subcommittee on Space and Aeronautics

Committee on Science, Space and Technology

U.S. House of Representatives

Statement by:
Jeff Seaton
Chief Information Officer (Acting)

116th Congress
HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
September 18, 2020

Statement of
Jeff Seaton
Chief Information Officer (Acting)
National Aeronautics and Space Administration

before the

Subcommittee on Space and Aeronautics
Committee on Science, Space and Technology
U.S. House of Representatives

Chairwoman Horn, Ranking Member Babin, and members of the Subcommittee, thank you for the opportunity to testify before you today about NASA's information technology (IT) infrastructure, and our efforts to manage and protect this infrastructure during the COVID-19 pandemic while enabling the vast majority of our employees and contractors to continue working remotely. Thankfully, due to strategic Agency investments in the NASA IT environment over the last several years, NASA was well positioned to quickly move its workforce to telework status in early March which not only kept NASA working, but also likely prevented greater exposure of our employees to the highly contagious COVID-19 virus. We are now in the process of returning to more on-site work, in a gradual manner, based on many factors including localized conditions, and guidance from the Centers for Disease Control and other Federal partners. The safety of our workforce remains our top priority. At the same time, protecting and effectively evolving NASA's IT infrastructure continues to be another top Agency focus.

As NASA's Acting Chief Information Officer (CIO), my office provides IT products and services, including policies and procedures for all of NASA. Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with space agencies around the world and have deep partnerships with researchers, engineers, academics, and scientists worldwide. Normally hundreds of thousands of NASA personnel, contractors, partners and members of the public access some part of NASA's IT infrastructure, a complex array of information systems with components geographically dispersed around the globe, on a daily basis. NASA's IT infrastructure plays a critical role in every aspect of NASA's mission, from enabling collaboration to controlling spacecraft to processing scientific data. In the President's FY 2021 budget request, the Agency has proposed to spend approximately $2.2B on enterprise, mission, and mission support IT products and services. NASA also recently received an additional $60M in emergency supplemental funding to help the Agency respond to the COVID crisis, with about one-third of that funding focused on IT capabilities.

Despite the pandemic, NASA remains fully committed to becoming more secure, effective and resilient, and we are actively pursuing these commitments at all levels. Today, OCIO's job is even more challenging with the vast majority of NASA's workforce – both civil servants and contractors – teleworking from remote locations across the country. Thus, enabling the NASA workforce to continue working in an environment that is very different from how we worked only a few months ago, has changed the demands on our IT infrastructure. The requirements and expectations on our IT capabilities and our OCIO teams are high, and the threats from external actors remain an ongoing concern. However,

with hard work, dedication, and innovation, the team I have the privilege of leading has risen to the challenge of keeping NASA's missions moving forward during these challenging times.

The OCIO team, including OCIO employees and contractors at all NASA Centers and facilities, continue to put in long hours, while also developing creative, innovative and secure solutions to new challenges as they arise. One such challenge was the need of NASA's medical community to trace interactions of the NASA workforce with employees who have been confirmed positive for COVID-19 while on-site at any NASA facility. The OCIO team helped develop software that simplified the process of contact tracing conducted by NASA health professionals to protect our workforce and mission while also protecting the privacy information of those exposed, meeting all relevant privacy laws. OCIO has also supported the need for senior leaders to visualize COVID-related data from multiple sources, including regional case-count trends near NASA facilities, thereby enabling senior leaders to make better-informed Return to On-Site Work (RTOW) decisions for each Center across the Agency. During this time, NASA employees as a whole have significantly increased their use of collaboration tools provided by the CIO such as Microsoft Teams and WebEx, as well as secure streaming video for virtual town halls and operational needs. With the support of OCIO, NASA also has continued to hire and onboard new employees and contractors, and to support summer interns with virtual learning opportunities, including providing them with the technology tools they need through both on-site and remote distribution. Even this testimony and various Agency meetings with Congressional Members and staff have been done remotely. During the pandemic, we have seen individuals and teams find new ways to keep the mission moving forward; to support each other; to balance work and family pressures; and even dedicate their expertise and personal time to partner with local companies to help develop technologies to help treat COVID patients and to better protect frontline responders. These are just a few of our success stories – many of which we've shared with other Federal partners. We also continue to learn from the telework experiences of other Federal agencies, fully recognizing that we are all in this together. My testimony today will touch on some of these successes, while also describing NASA's remote work journey, addressing how we are responding to increased requirements on and threats to our IT infrastructure during the pandemic – themes that are common to many Federal agencies.

Responding to a Pandemic

As signs of a nationwide pandemic developed in early February 2020, NASA senior leaders began to use the Agency's Continuity of Operations Plan (COOP) to assess capabilities and conditions at Agency locations and determine when it would be appropriate to proactively begin moving employees into a telework status due to the increasing spread of the virus. Then in early March, NASA conducted an Agency-wide telework exercise to stress test NASA's IT capabilities needed to support massive teleworking. During that exercise, we saw a 300 percent increase in single-day telework users and associated increases in the utilization of our remote IT infrastructure, and our IT systems effectively supported this increased load. Shortly after this exercise, in mid-March, Agency senior leaders began making the difficult decisions to move nearly the entire workforce, Center-by Center based on local conditions, into a telework status. Only a limited number of employees performing mission-critical work requiring on-site access for the protection and safe operation of critical Agency infrastructure and a few select missions (e.g., DM2 launch and Mars Perseverance preparations) were initially authorized to be on-site, following clearly defined health and safety protocols. Thus, NASA has never been "closed." On the contrary, our employees continued to perform NASA's important missions under very difficult personal and professional circumstances, leveraging technology and communication tools to continue a majority of NASA's work. More than 90 percent of the NASA workforce was in a telework status by the end of March 2020. Today, about 75 percent of employees and contractors are continuing to work remotely, with the amount varying by mission requirement and location.

NASA is currently using a NASA-developed RTOW Framework[1] to safely increase the amount of work being done on-site at our Centers and facilities. Increased levels of RTOW will be gradual as local conditions at each NASA Center/facility become safer to return. NASA also has strict safety protocols in place for employees who are returning to on-site work, including requiring all employees (civil servant and contractor) and anyone else who enters a NASA facility to wear face masks when they cannot ensure appropriate social distancing. NASA Centers and facilities are also using temperature checks as a health screening tool, and NASA continues to investigate other technologies that may provide protections for our workforce. Should an employee who has been on-site test positive for COVID-19, NASA has a contact tracing protocol to identify and notify others who may have been exposed to an infected person. NASA then requires infected and exposed persons to self-quarantine, and we have aggressive cleaning protocols for impacted areas. NASA also continues to actively communicate with other Federal agencies about how we are responding to the COVID crisis and to share best practices with them, while also learning from the successes of others.

During these challenging times, NASA senior leadership continues to put our employees first by maximizing flexibilities for employees to perform their NASA work while also enabling them to care for themselves and their families. Leave and telework flexibilities consistent with Office of Personnel Management (OPM) guidance are available to employees, including limited paid leave for care of young children. We also have encouraged our supervisors to provide the greatest amount of flexibility in what hours employees work., e.g., allowing them to change start/stop times or to break up their eight-hour workdays into sections to better accommodate their family needs at home. For my part, even with the increased demands on our IT workforce, I am challenging my team leaders to set the example and take time off to recharge and take care of themselves and their families. We're also encouraging employees to "unplug" and take breaks, which admittedly can be difficult when you work in OCIO and have to keep the Agency's IT infrastructure performing securely 24 hours a day, 7 days a week. NASA also continues to keep our workforce informed about RTOW plans via emails from senior leaders, virtual townhall events, and Agency-wide and Center-specific websites.

The NASA Telework Experience

Over the last several years, NASA has invested significantly in modernizing our network, collaboration tools, and cybersecurity capabilities that are critical to enabling NASA team members to effectively work both on site and remotely. We've also conducted multiple Center and Agency telework exercises to test our systems and to learn from and resolve any issues. The lessons we've learned through our COOP and telework exercises enabled us to rapidly and seamlessly transition into what has become an extended telework environment. Even before the pandemic, the NASA OCIO was analyzing ways to allow for our employees to securely work remotely from any location due to the increasingly mobile nature of our workforce. For many years, NASA has been moving from stand-alone desktops to mobile laptops to support the way in which distributed, mobile teams work. Many employees travel occasionally and/or bring their laptops home with them often – even daily – in case of weather events or other emergencies, or simply to do work in the evening. NASA also supports routine telework. With supervisor approval, it was not unusual for some employees to telework one or two days a week even prior to the pandemic. While some work must always be performed on site, the NASA team has been incredibly productive over the past several months of largely remote work and we are already using the lessons we have been learning during the pandemic to add to our ongoing "Future of Work" planning – a NASA effort where OCIO is playing a key role in helping to define NASA's future work environment.

[1] The following website includes specifics about our RTOW plans; including a copy of our RTOW Framework; a list of Frequently Asked Questions and Answers; and a list of the each Center's operational status: https://nasapeople.nasa.gov/coronavirus/coronavirus.htm.

With most of the NASA workforce teleworking during the pandemic, there are greater risks to NASA data when accessed remotely as opposed to being on site with a direct Agency network connection. To address the increased risks associated with remote work, several years ago, NASA began protecting information on Agency laptops with Data At Rest encryption software. Additionally, NASA IT users who are working remotely are required to use the NASA Virtual Private Network (VPN) when connecting to internal NASA systems. Additionally, NASA OCIO has authorized some missions to host their own VPNs, which allows defined limited connectivity to external partners, thus enforcing segregation our partners and their systems from NASA's internal systems.

Pre-pandemic enhancements to NASA's remote infrastructure also aided its response to the present pandemic. In early 2019, NASA OCIO upgraded the Agency's VPN infrastructure, expanding capacity from 24,000 to more than 55,000 concurrent users. Additionally, NASA OCIO made improvements to its network architecture to add additional resiliency, redundancy, and increased bandwidth. At the height of teleworking during the pandemic, where NASA saw about 90 percent of the workforce connecting remotely, an average of more than 37,000 civil servants and contractors were using the Agency's VPN each day, with the maximum utilization exceeding 40,000 users in a single day. Prior to the pandemic, the most connect ions to the NASA VPN on a single day was less than 12,000. While there have been some minor network and connectivity issues that have required additional architecture and configuration changes during the pandemic, and while we cannot address home and local network issues, the NASA network and VPN infrastructure has performed extremely well, with a measured 99.85 percent availability since the start of the remote telework period.

When working remotely, employees can respond to phone calls via NASA-provided mobile data devices, or by calling into a voicemail system and retrieving messages. In addition, NASA is using a softphone application installed on employee laptops that allows users to use their computers to make and receive phone calls over the network as if using their office telephone. Email and official documents sent on NASA-provided mobile devices are also secured via NASA's mobile device management software which provides secure storage and encrypted mobile connection to NASA mobile applications, including email and scheduling.

During the pandemic, NASA employees have capitalized on new ways to virtually connect and collaborate via tools such as Microsoft Teams, which OCIO finished deploying across NASA in October 2019 as part of the Agency's migration to the Microsoft Office 365 cloud-based suite of tools. While some employees adapted to the new collaboration tools immediately, use of these new capabilities really grew rapidly once NASA employees began working remotely, because they suddenly had a need to conduct meetings and have conversations with colleagues that were also remote. In fact, the video and chat capabilities became such a critical tool for the entire NASA workforce that NASA's use of Teams increased more than 300 percent since March to nearly 38,000 daily active users, and this way of virtually working via video has now become the norm. An additional response to the pandemic-related collaboration needs included NASA's CIO team integrating audio dial-in capabilities with Teams meetings beginning in April, replacing the need for many traditional, external conference-call lines. This audio integration also supported the accessibility needs of the workforce by allowing interpreters to use the dial-in functionality during meetings. As of August, NASA has approximately 9,000 employees using the new Teams audio-conference capability, providing them access to virtual team meetings even if their only access is a mobile phone. In parallel, OCIO expedited the release and availability of mobile Office 365 applications for NASA-managed mobile phones, so that employees can also connect to Teams meetings and access video and chat from their mobile phones via a Wi-Fi or cellular data connection, making many employees truly mobile NASA workers. Also, the recent addition of live captioning to Teams meetings further expanded the accessibility capabilities provided to NASA employees.

Providing new and replacement equipment and effective remote support has been essential to sustaining the productivity of the remote NASA workforce during the pandemic. To address these challenges, NASA OCIO developed and implemented a process to ship IT equipment (laptops, cell phones) to new employees, as well as replacement hardware to current employees experiencing technical difficulties and system failures, and established processes to set up, configure, and remotely troubleshoot hardware and software remotely. These processes have allowed employees to remain safely at home and avoid visits to a NASA Center to resolve technical issues in person, although on-site support is also available when needed. OCIO also partnered with the Office of Protective Services (OPS) to implement a secure approach to remotely process personal identity verification (PIV) badge renewals and replacements utilizing the expanded collaboration capabilities, again allowing employees to avoid travelling to a NASA Center unnecessarily. This activity involved collaboration with multiple offices including OPS and the Office of the Chief Human Capital Officer. Additionally, OCIO increased staffing at IT help desks to assist employees who were experiencing technical difficulties, in most cases, completely virtually.

NASA IT Threat Environment

Like other Federal agencies, NASA's IT infrastructure is under constant attack from domestic and foreign adversaries. Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals, and foreign enterprises. Many of these threats are well-resourced, highly motivated, and sophisticated – and those threats have not gone away during the pandemic. Unfortunately, there is no perfect, one-size-fits-all approach or technology to predict, counter, and mitigate the wide range of cyber attacks across the Federal Government. To address this dynamic threat landscape, NASA continues to strengthen our technical and procedural capabilities to attain situational awareness and proactively defend the IT assets supporting our enterprise, including those assets that are outside the traditional borders of the NASA network.

The collective actions of the NASA OCIO team, as well as information sharing with the Department of Homeland Security (DHS) and other Federal agencies involved in cybersecurity, are contributing to an improved IT security posture at NASA. When threats are detected, NASA personnel take immediate action and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks. Today, for example, NASA is a leader in the adoption of DHS's Continuous Diagnostics and Mitigation (CDM) program, which enables NASA to identify assets and vulnerabilities across our network and implement plans for remediation of issues. We have partnered with other agencies that have deployed CDM to ensure we can transfer our knowledge to them, and receive lessons learned from other agencies. Deployment of CDM Phase 1, which focuses on identifying what is on NASA's networks, is now complete across our corporate network and NASA is making significant progress on the mission network, with completion scheduled for the fourth quarter of FY 2021. OCIO has successfully implemented CDM Phase 2, which included identifying "who" is on NASA's network along with privilege access. For CDM Phase 3, which focuses on "network security management" is being worked with DHS as part of the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) contract. OCIO is currently on schedule with DHS in its deployment of technologies to monitor unauthorized IT device connections designed to remove or block these devices from accessing NASA's networks and systems. OCIO's initial enforcement implementation for the corporate network is scheduled for the second quarter of FY 2021. While NASA's cybersecurity efforts will never be "done," significant progress has been made recently. OCIO's efforts to better secure NASA data and systems have resulted in NASA achieving a rating of "Managing Risk," which is the highest rating, on the two most recent Federal Information Security Management Act (FISMA) framework assessments.

In order to address the unique cyber risks and challenges posed by human spaceflight, and in particular by NASA's Artemis Program, OCIO also has partnered with the Human Exploration and Operations Mission Directorate (HEOMD) and its Advanced Exploration Systems Division at Headquarters. A senior OCIO staff member is engaged in program planning and leadership meetings, providing immediate OCIO input on relevant cybersecurity and programmatic matters. This partnership allows OCIO to better understand HEOMD's programs, processes, and mission requirements while helping HEOMD leadership identify and resolve any cybersecurity gaps by evaluating cybersecurity requirements, ensuring an integrated approach to addressing cybersecurity risks, and making certain that cybersecurity considerations are included at the outset of this groundbreaking work. In addition to OCIO's partnership with HEOMD, OCIO continues to proactively work with other NASA projects and missions to strengthen mission cybersecurity and to support emerging IT requirements.

Over the last several years, NASA has also made great strides in PIV efforts, requiring 100 percent of privileged users to authenticate with PIV, and between FY 2017 and FY 2019, increasing the percentage of unprivileged users required to use PIV from 72 percent to 90 percent over that period. NASA has developed PIV solutions for a variety of unique NASA systems and CDM efforts, including developing the first-ever native smartcard authentication for Apple's MacOS platform, a solution which NASA has shared with other Federal partners and further solidifying the security of identity management and access on the Agency's network. Because of these efforts, NASA's Identity, Credential and Access Management (ICAM) program was a finalist for the National Security Agency's prestigious Frank B. Rowlett Award, which recognizes outstanding Federal Government excellence in the field of cybersecurity. This has helped NASA achieve the "Managing Risk' (highest score) under the FISMA framework.

To further strengthen NASA's existing Security Operations Center (SOC), in FY 2020, NASA developed a SOC COOP capability. Previously, if cybersecurity operations at NASA's Ames Research Center were disrupted, the Agency would have been limited in its ability to identify, detect, and respond to cybersecurity incidents. With the new SOC back-up operations and processes in place concurrently across multiple Centers, NASA is prepared to maintain SOC operations in the event of an isolated disruption. The development of the SOC COOP was accompanied by an increase in NASA's overall SOC capabilities as well, moving the NASA SOC from a predominately reactive capability to a pro-active resource supporting the Agency's cybersecurity needs. As the pandemic spread in April, 2020, NASA OCIO made the decision to activate our previously-established and tested COOP plan and moved our 24x7 network operations center which manages NASA's critical administrative network infrastructure to a remote operations posture to ensure the safety of NASA's essential network management personnel without impacting services. In this demanding environment, the NASA CIO team has continued to effectively manage and protect NASA's IT infrastructure, largely in a remote manner. On occasions when employees are required to be onsite to support critical SOC or network operations activities, we have followed NASA processes to maintain appropriate social distancing, wear masks as required, and follow all other facility-access requirements.

Despite OCIO's increased workload during the pandemic, the OCIO team also has continued to make progress on several key network and cybersecurity initiatives. For example, to support large, virtual meetings, OCIO deployed a secure, PIV-enabled streaming video service in less than 60 days to support NASA management's need to engage in live communication with employees.

Looking Ahead

Effective IT management in a complex environment like NASA is not an easy task even under normal circumstances. Investment decisions must balance multiple stakeholder and mission requirements, cybersecurity risk management, and the rapid pace of technology development to allocate available

resources to the highest priority IT investments that will best enable mission success. Additionally, like all Federal agencies, NASA is adjusting to new laws and directives designed to improve how the entire Federal Government manages and secures its IT resources. While NASA is proud of the progress we have made, we recognize that more work remains as we strive to effectively and efficiently manage our IT resources, modernize out IT environment, all the while complying with ever-changing laws and policy. There is a lot at NASA to be excited about, and as the Acting CIO, I am encouraged by the continual support the CIO receives from NASA leadership as well as the partnership role the CIO plays in key decision-making processes within the Agency. Here are just a few of the exciting opportunities ahead of the NASA OCIO team:

- **Cloud Computing and Backup:** NASA's commercial cloud computing interest and adoption has rapidly escalated as missions are aggressively making the transition from traditional Agency-hosted software platforms to reliance on cloud-native services and applications. There is also significant interest in delivering observation data from orbiting assets directly to the cloud. NASA is presently consuming more than 1.8M computing hours in the commercial cloud every month and has almost 10 petabytes of data stored in the cloud, with the majority of data available for unrestricted use by the global science community. The portfolio of data for just one major NASA program will increase this data amount by at least an order of magnitude within the next five years. Mission growth in the use of commercial cloud computing services is fully aligned with the Agency's thrust to rely on industry as much as possible for capabilities so that NASA can focus on its key objectives in the areas of science and discovery. Additionally, OCIO is implementing an Agency-wide Cloud Backup Solution in order to seamlessly protect, back up, and restore files across any organization or user, regardless of device or location, from a secure, cloud architecture, a capability that also further protects NASA from growing cyber threats such as ransomware attacks.
- **Website Consolidation and Modernization:** NASA OCIO is also collaborating on a full assessment of NASA's web footprint and digital presence through the NASA Website Modernization Team, which will deliver an enhanced cyber posture, improved operating efficiencies, and a strengthened focus for publicly communicating the inspiring messages and amazing data coming from NASA missions. This is a priority for NASA's senior leadership, as outlined in a May 15, 2019, memo from NASA Administrator James Bridenstine.
- **Digital Transformation:** As part of the NASA CIO's efforts in IT modernization, OCIO is helping to drive the concept of digital transformation across NASA in areas such as collaboration, artificial intelligence and machine learning, cloud computing, big data, and robotic process automation.

Conclusion

In conclusion, NASA is continuing to execute a diverse portfolio of exciting and challenging missions on a daily basis, even with a significant percentage of the NASA team continuing to primarily operate in a remote work environment today. While we are unsure what the future holds in terms of an end to this global pandemic, NASA senior leaders, including myself, are committed to keeping the NASA workforce safe and to providing them with the tools and IT infrastructure they need to continue to successfully execute their missions while working remotely as we gradually return to on-site work. At the same time, I want to assure you that protecting and evolving NASA's IT infrastructure is and will remain a top Agency priority. Thank you for the opportunity to testify before you today and for your continued support of NASA's missions and our people. I would be happy to answer any questions you may have.

Jeff Seaton
NASA Chief Information Officer (Acting)

Jeff Seaton is NASA's Chief Information Officer (Acting). Prior to this appointment, he served as Deputy Chief Information Officer. Seaton came to NASA Headquarters from NASA's Langley Research Center, where he was Chief Information Officer from 2011 to 2018. During that time, he was also a member of the NASA Langley Senior Staff and the Agency's CIO Executive Council. Jeff led transformative change efforts in both the Langley and CIO enterprise across the Agency to increase effectiveness and accountability of the services provided by the organization.

Jeff began his career with NASA in 1991 as a research engineer designing robotic systems for use in space-based applications. He also conducted research in the field of computer vision techniques applied to the control of robots. Jeff was a member of NASA's 2008 Senior Executive Service Candidate Development Program and served as Langley's Chief Technology Officer and Deputy Chief Information Officer prior to becoming CIO.

In addition to his CIO duties, Jeff was a member of the Business Services Steering Committee charged with identifying opportunities for NASA to improve the efficiency and effectiveness of all mission support services. He was also the executive champion of the Langley Emerging and Advancing Professionals employee resource group, has led Langley's digital transformation efforts, and helped to lead Langley's High Performance Computing Incubator. He has received numerous awards for his service to the Agency, including NASA's Outstanding Leadership Medal in 2014.

Chairwoman HORN. Thank you very much, Mr. Seaton. Mr. Martin, recognized—you are now recognized for your testimony.

TESTIMONY OF THE HONORABLE PAUL K. MARTIN, INSPECTOR GENERAL, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Mr. MARTIN. Thank you, Chairwoman Horn, Ranking Member Babin, and Members of the Subcommittee. The NASA Office of Inspector General has conducted a significant amount of oversight work to help NASA improve its information technology governance, while securing its networks and data from cyber attacks. Over the past 5 years we issued 16 audit reports, with 72 recommendations related to IT governance and security. During this same period we've conducted more than 120 investigations involving intrusions, denial of service attacks, and data breaches on NASA networks, several of which have resulted in criminal convictions. My testimony today is informed by this body of audit and investigative work.

The soundness and security of its data and IT systems is central to NASA's success. The agency spends more than $2.2 billion a year on a portfolio of IT assets that include hundreds of information systems used to control spacecraft, collect and process scientific data, and enable NASA personnel to collaborate with colleagues around the world. Given the valuable technical and intellectual capital NASA produces, its IT systems present a high value target for cyber criminals. The past 6 months in particular has tested the agency, as more than 90 percent of NASA's workforce moved from onsite to remote work due to the pandemic. During this period, NASA has experienced an uptick in cyber threats, with phishing attempts doubling, and malware attacks rising substantially. This morning I offer three observations about the state of NASA's IT security and governance to provide context for the scope of its challenges.

First, our concerns with NASA's IT governance security are wide-ranging and longstanding. For more than 2 decades NASA has struggled to implement an effective IT governed structure that aligns authority and responsibility commensurate with the agency's overall mission. Specifically, the agency's CIO has limited oversight and influence over IT purchases and security decisions within mission directorates and at NASA centers. This de-centralized nature of NASA's operations, coupled with its historic culture of autonomy, have hindered the CIO's ability to implement effective enterprise-wide IT governance. Moreover, NASA's connectivity with educational institutions, and other outside organizations, and its vast online presence of 3,000 web domains, and more than 42,000 publicly accessible data sets, offer cyber criminals a larger target than most other government agencies.

Second, despite positive forward momentum, the agency's IT practices continue to fall short of Federal requirements. For example, in 2019, for the fourth year in a row, NASA performance during our annual *FISMA* review remained at level two out of five, meaning the agency has issued, but has not consistently implemented, important policies and procedures defining its IT security program. And third, like many other public and private organiza-

tions, NASA struggles to find the right balance between user flexibility and system security. For example, for years NASA permitted personally owned and partner owned mobile IT devices to access non-public data, even if those devices did not have a valid authorization. Today NASA employees and partners can use non-agency mobile devices to access e-mail if the user installs security software known as mobile device management.

However, an OIG (Office of Inspector General) audit last month found that NASA was not adequately securing its e-mail networks from unauthorized access by these personally owned devices. Although NASA has deployed technologies to monitor unauthorized connections, it has not fully implemented controls to remove or block those devices. Moreover, the agency's December 2019 target for installing these controls was delayed due to technological issues and pandemic-related center closures. Until these enforcement controls are fully implemented, NASA faces an elevated risk of a breach.

Finally, as part of its MAP (Mission Support Future Architecture Program) initiative, NASA plans to centralize and consolidate IT capabilities. The CIO's office expects to complete its MAP assessment by March 2021, with implementation on its institutional systems beginning later that year. As MAP unfolds, we plan to assess whether this enterprise-level alignment has strengthened cybersecurity at NASA. I look forward to your questions.

[The prepared statement of Mr. Martin follows:]

NASA
National Aeronautics and Space Administration

Office of Inspector General

Testimony before the House of Representatives
Subcommittee on Space and Aeronautics,
Committee on Science, Space, and Technology

CYBERSECURITY AT NASA: ONGOING CHALLENGES AND EMERGING ISSUES FOR INCREASED TELEWORK DURING COVID-19

Statement of Paul K. Martin
Inspector General
National Aeronautics and Space Administration

For Release on Delivery (expected at 11 a.m.)
September 18, 2020

Chairwoman Horn, Ranking Member Babin, and Members of the Subcommittee:

The Office of Inspector General (OIG) is committed to providing independent, aggressive, objective oversight of NASA programs and projects, and we welcome this opportunity to discuss the Agency's challenges with improving its information technology (IT) governance while securing its networks and systems from cybersecurity attacks, particularly during a period when the vast majority of NASA employees and many contractors are teleworking due to the pandemic.

The soundness and security of NASA's data and IT systems is central to the success of its space exploration, science, and aeronautics goals. The Agency spends more than $2.2 billion a year on a portfolio of IT assets that include hundreds of information systems used to control spacecraft, collect and process scientific data, provide IT infrastructure security, and enable NASA personnel to collaborate with colleagues around the world. The Agency's Office of the Chief Information Officer (OCIO) is responsible for helping to protect the confidentiality, integrity, and availability of data and information systems and has oversight of some but not all of NASA's IT investments. OCIO manages the institutional IT systems throughout the Agency, and in FY 2020 allocated $74 million to cybersecurity.[1]

Given NASA's mission and the valuable technical and intellectual capital it produces, the Agency's IT infrastructure presents a high-value target for hackers and cyber criminals. The past 6 months in particular have tested the Agency's ability to manage its IT systems and maintain adequate security as more than 90 percent of NASA's workforce has moved from on-site to fulltime remote work due to the COVID-19 pandemic.

Consistent oversight of NASA's IT governance and security challenges remains a top priority for the OIG. Over the past 5 years, the OIG has issued 16 audit reports containing 72 recommendations related to IT governance and security, including evaluations of the Agency's information security program, the use of non-Agency IT devices to conduct Agency business, and cybersecurity management and oversight.[2] In addition, during the past 5 years OIG investigators conducted more than 120 investigations involving intrusions, malware, denial of service attacks, and data breaches on NASA networks, several of which have resulted in criminal convictions. My testimony today is informed by this body of audit and investigative work.

IT Governance and Security

Our concerns with NASA's IT governance and security are long-standing and reoccurring. For more than two decades, NASA's OCIO has struggled to implement an effective IT governance structure that aligns authority and responsibility commensurate with the Agency's overall mission. Specifically, we have found that the Agency Chief Information Officer (CIO) and IT security officials have limited oversight and

[1] NASA's IT assets generally fall into two broad categories: institutional and mission. Institutional (corporate) systems support the day-to-day work of NASA employees and include networks, data centers, web services, desktop and laptop computers, enterprise business applications, and other end-user tools such as email and calendars. Mission systems support the Agency's aeronautics, science, and space exploration programs and host hundreds of IT systems distributed throughout the United States.

[2] NASA OIG audit reports are available at https://oig.nasa.gov/audits/auditReports.html.

influence over IT purchases and security decisions within Mission Directorates and at NASA Centers.[3] The decentralized nature of NASA's operations coupled with its long-standing culture of autonomy hinder the OCIO's ability to implement effective enterprise-wide IT governance. For example, in an August 2020 audit we found OCIO's visibility into the process Centers use to authorize and approve IT systems and devices to access Agency networks remains limited.[4] Although the NASA CIO is responsible for developing an Agency-wide information security program, OCIO relies on Center-based CIOs and IT security staff to implement and enforce the Agency's information security policies. This practice has allowed Centers to tailor processes to meet their own priorities, which has in turn led to inconsistent implementation of NASA's enterprise-wide IT security management. Such a decentralized approach to cybersecurity management limits OCIO's ability to effectively oversee NASA's information security activities and make informed decisions related to project timelines, costs, and efficiencies as well as realistically assess the overall security of NASA's numerous IT systems.

Furthermore, despite some positive forward momentum, the Agency's IT practices continue to fall short of federal requirements. For example, in July 2020 NASA received an overall grade of C+ from the U.S. House of Representatives Committee on Oversight and Reform on the most recent Federal Information Technology Acquisition Reform Act (FITARA) scorecard due to issues with managing major IT investment risk and cyber threats.[5] Additionally, in 2019 for the fourth year in a row, NASA's performance during our annual Federal Information Security Modernization Act (FISMA) review remained at a Level 2 out of 5—meaning the Agency has issued, but has not consistently implemented, policy and procedures defining its IT security program—well short of standards set by the Office of Management and Budget (OMB) for an effective agency-wide information security program.

In our June 2020 FIMSA report, we found system security plan documentation for all six information systems we reviewed contained numerous instances of incomplete, inaccurate, or missing information.[6] We also performed a limited review of the Agency Common Control (ACC) system that aggregates and manages common security controls across all Agency information systems and found that many were classified as "other than satisfied," indicating they had been assessed as less than effective. Moreover, to date the NASA OCIO has not addressed deficiencies in the ACC system security plan. At NASA, Chief Information Security Officers (CISO) at each Center are responsible for providing oversight to ensure system security plans and related security information are documented in the Agency's Risk Information Security Compliance System (RISCS). However, system security plan weaknesses occurred because CISO's often are responsible for managing large portfolios of information systems and do not have resources available to ensure data in RISCS for each system is accurate and complete and the OCIO does not consistently require the use of RISCS as the Agency's information security management tool.

Further, we reported that NASA information security personnel were not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that

[3] NASA consists of a Headquarters office in Washington, D.C.; nine geographically dispersed Centers; the Jet Propulsion Laboratory, a federally funded research and development center operated under contract by the California Institute of Technology; and nine component facilities and testing sites such as the Katherine Johnson Independent Verification and Validation Facility and the White Sands Test Facility. The Agency's four Mission Directorates include Aeronautics Research; Human Exploration and Operations; Science; and Space Technology.

[4] NASA OIG, *NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices* (IG-20-021, August 27, 2020).

[5] FITARA scorecard - July 2020.

[6] NASA OIG, *Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019* (IG-20-017, June 25, 2020).

delinquent information security assessments are identified and mitigated. As a result, information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA information. Of the six information systems reviewed, we found that four were operating without current contingency plans. NASA policy requires information system owners to review contingency plans for accuracy and completeness at least annually or when significant changes are made. Additionally, authorizing officials responsible for reviewing and approving information systems do not regularly test to determine whether the information in RISCS is accurate and available for senior IT leadership. Moreover, the number of systems with out-of-date or nonexistent contingency plans in RISCS puts NASA at an unnecessarily high risk and hinders the Agency's ability to effectively and efficiently recover information systems if they crash or are compromised, thus threatening the confidentiality, integrity, and availability of the information maintained in those systems.

In a separate March 2020 report, we examined NASA's management of Distributed Active Archive Centers (DAACs) and found that NASA deviated from recommended National Institutes of Standards and Technology (NIST) guidelines when determining what information types to include in system descriptions.[7] Accurate system categorization is critical to determining the level of protection a system requires. In our audit, we found critical information types such as environmental monitoring and forecasting were excluded when conducting impact determinations. This occurred because NASA and NIST categorization guidance was misinterpreted by the system owners—mission and project personnel—due to a lack of close OCIO involvement.[8] Failure to appropriately categorize systems and data can result in inadequate controls for protecting the confidentiality, integrity, and availability of the system and its data.

Securing NASA IT Systems

For almost 20 years we have identified securing NASA's IT systems and data as a top management challenge.[9] This year in particular NASA has experienced an uptick in cyber threats: phishing attempts have doubled and malware attacks have increased exponentially during the COVID-19 pandemic. Given its vast online presence of approximately 3,000 web domains and more than 42,000 publicly-accessible datasets, the Agency is highly vulnerable to intrusions. To help ameliorate this vulnerability, the NASA Office of the Chief Scientist is leading a team to review NASA's web footprint and digital presence to recommend ways to strengthen digital security and reduce cyber vulnerabilities.[10]

Given its mission, the Agency's 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. For example, in 2019 following a joint investigation by the OIG and the Defense Criminal Investigative Service, two Chinese nationals were indicted on criminal charges for gaining unauthorized access to a NASA computer to steal data. In addition, each NASA Center and

[7] Located at NASA Centers, universities, and other federal agencies, DAACs process, archive, and distribute data; NASA OIG, *NASA's Management of Distributed Active Archive Centers* (IG-20-011, March 3, 2020).

[8] To help ensure data processed by a DAAC is adequately protected, NIST provides guidance for system categorization, including a library of information types with recommended impact levels, to determine whether a system should operate at a low, moderate, or high impact level.

[9] NASA OIG Top Management and Performance Challenges reports are available at https://oig.nasa.gov/challenges.html.

[10] A "digital presence" refers to how NASA appears online. For example, digital presence includes not only content the Agency controls such as its websites and social media profiles, but also content it cannot control such as online reviews or comments. NASA Administrator, *Web Site Modernization and Enhanced Security Protocols*, May 15, 2019.

the Jet Propulsion Laboratory (JPL) are frequent targets of cybersecurity attacks. For example, in 2011 cyber intruders gained full access to 18 servers supporting key JPL missions and stole 87 gigabytes of data. More recently, in April 2018 JPL discovered that an account belonging to an external user had been compromised and used to steal approximately 500 megabytes of data from a major mission system.

These and similar incidents prompted our office to conduct an audit to assess the effectiveness of JPL's network security controls for externally facing applications and systems. In June 2019, we reported that the IT security database JPL uses to track and manage physical assets and applications on its network was incomplete and inaccurate, placing at risk JPL's ability to effectively monitor, report, and respond to security incidents.[11] Moreover, poor visibility into devices connected to its networks hinders JPL's ability to properly secure those networks. This shortcoming enabled an attacker to gain unauthorized access to JPL's mission network through a compromised external user system (the example cited above). Additionally, the review found NASA failed to establish Interconnection Security Agreements to document the requirements partners must meet to connect to NASA IT systems.

We also found that security problem log tickets, created in JPL's IT security database when a potential or actual IT system security vulnerability is identified, were not resolved for extended periods of time—sometimes longer than 180 days. Further, JPL system administrators misunderstood their responsibilities regarding management and review of logs for identifying malicious activity occurring on a system or network. Moreover, we found that while cybersecurity monitoring tools employed by JPL defend against routine intrusions and misuse of computer assets, JPL had not implemented a threat hunting program recommended by IT security experts to aggressively pursue abnormal activity on its systems for signs of compromise, and instead relied on an ad hoc process to search for intruders. JPL had also not provided role-based security training or funded IT security certifications for its system administrators. Finally, while the contract between NASA and the California Institute of Technology (Caltech)—the entity that operates JPL—requires JPL to report certain types of IT security incidents to the Agency, we found no controls in place to ensure compliance with this requirement.

Despite these significant concerns, the contract NASA signed with Caltech in October 2018 to manage JPL for at least the next 5 years left important IT security requirements unresolved and instead both sides agreed to continue negotiating these issues. For example, the contract did not include relevant requirements from NASA IT security policies or resolve disagreements between NASA and Caltech regarding the implementation of Continuous Diagnostics and Mitigation at JPL, transitioning JPL systems from the government domain to a private domain, and establishing compliance of JPL websites with relevant regulatory requirements including FISMA. In January 2020, after reviewing JPL's IT Transition Plan required by the contract that outlined the implementation of continuous monitoring tools and IT security practices, we determined that our concerns had been addressed.

Ensuring secure access to the Agency's non-public networks and systems also remains a high-level IT security concern. Smartphones, tablets, and laptops are integral to the work of tens of thousands of NASA employees and contractors, academic, federal, and international partners; however, use of this equipment to connect to non-public NASA networks and systems increases opportunities for improper access to Agency data. Like many other public and private organizations, NASA continues to struggle to find the correct balance between user flexibility and system security. For years, NASA permitted personally-owned and partner-owned IT devices to access non-public data through its networks and systems, even if those devices did not have a valid authorization. Even though NASA policy since 2006

[11] NASA OIG, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory* (IG-19-022, June 18, 2019).

specifically prohibited such unauthorized devices to access its networks and systems, the policy was not consistently enforced. However, in April 2018 the CIO specifically disallowed connection of personally-owned and partner-owned IT devices to NASA networks or systems, deeming them "unauthorized devices." That decision prompted significant pushback from NASA employees and partners resulting in a follow-up memorandum in October 2018 that established new requirements allowing NASA employees and partners to use personally-owned mobile devices to securely access the Agency's enterprise email system if the user installed security software known as a Mobile Device Management (MDM) application.

However, our August 2020 audit of these issues found that NASA was not adequately securing its networks from unauthorized access by personally owned mobile devices.[12] Although OCIO had deployed technologies to monitor unauthorized IT device connections, it had not fully implemented controls to, when needed, remove or block these devices from accessing NASA's networks and systems. The Agency's December 2019 target date for installation of these controls was delayed due to technological challenges and changes in OCIO mission priorities and requirements. Moreover, on-site work restrictions associated with the Agency's closure of its Centers and support facilities in response to the COVID-19 pandemic has negatively impacted the implementation schedule related to network access controls. Until these enforcement controls are fully implemented, NASA faces an elevated risk of a breach due to cybersecurity attacks.

We also noted that while the OCIO had established a process to implement MDM on employee and contractor personal mobile devices, it was not adequately monitoring and enforcing the business rules necessary when granting such access. For example, NASA did not adequately assess whether users accessing its email system had a business need to use a personal mobile device or if the mobile device was ineligible for participation in the MDM service because it violated supply chain controls—all of which increases the risk of the device being exploited. Additionally, while Agency personnel that have MDM installed on their personally-owned mobile device are not permitted to access the MDM service while outside the U.S. and its territories, we found the OCIO is not monitoring or enforcing this prohibition. As a result, NASA data is at increased risk from the use of unauthorized devices, which could expose the Agency to viruses, malware, or data loss.

Our investigative work has also identified issues with NASA's ability to properly protect personally identifiable information. For example, in November 2019 we issued a Management Referral regarding the compromise of a NASA system hosting more than 40,000 records containing personally identifiable information such as social security numbers and dates of birth. These records were improperly accessed when an Internet-facing server at a NASA Center was compromised and the attackers remained undetected for nearly a month after the intrusion. This attack—suspected to have originated from a Chinese IP address—occurred because of NASA's failure to apply a software patch in a timely fashion and inadequate monitoring. If not for notification by NASA counterintelligence officials, it is unclear when the intruders would have been detected through existing NASA cybersecurity processes and capabilities. As a result of this incident, NASA paid approximately $150,000 to a credit monitoring company for identity theft monitoring services for the affected employees.

Securing information technology is a continuous challenge across the Agency, including at the OIG. In fall 2019, we discovered evidence of a potential cyberattack on an OIG network and partnered with United States Computer Emergency Readiness Team to investigate the incident. Although we subsequently determined that no sensitive data had been compromised, that outcome likely was more

[12] IG-20-021.

due to luck than our security efforts. In response to the incident, the OIG has established a security oversight committee, improved automated security and software patching processes, and is pursuing an outside assessment of our overall IT system security.

Progress Addressing Challenges

NASA has taken a variety of actions to improve its IT governance structure over the past few years such as revising its governance boards; updating board charters; defining the roles and responsibilities of positions within the OCIO IT structure; and hiring four senior leadership positions in IT security, including a Senior Agency Information Security Officer. Additionally, in September 2019 NASA updated its IT Strategic Plan, which identifies critical activities, milestones, and resources needed to manage IT as a strategic resource. For example, consistent with the plan and past OIG recommendations, NASA streamlined its previously fragmented IT governance model by including executive members from each of the Mission Directorates and Centers on IT councils to assist with strategic IT decisions.

NASA has also taken steps to improve its overall security posture, including making progress in implementing cybersecurity initiatives and increasing Security Operations Center capabilities. For example, NASA developed a remedial action process and maintains a database to track the status of corrective actions for identified security vulnerabilities. However, while the initiative shows progress, as of May 2020 the database had more than 1,800 open actions. Agency officials attribute these delays to operational priorities and resource constraints. Additionally, NASA continues to make progress with identity management and authentication to provide increased visibility into who and what is connected to the Agency's institutional network although significant gaps remain, as evidenced in our August 2020 report.[13]

To further improve its operations, the OCIO is participating in the Mission Support Future Architecture Program (MAP) and is moving toward an enterprise computing model to centralize and consolidate IT capabilities while ensuring local requirements are met.[14] The OCIO expects to complete its MAP assessment by March 2021, with implementation beginning later that year. As MAP progresses, we will continue to assess whether this enterprise-level alignment has strengthened cybersecurity throughout the Agency.

Over the years, the OIG and OCIO have worked together cooperatively to improve NASA's IT security and governance. Of the 72 recommendations for improvement we made in the last 5 years, 46 have been closed with appropriate implementation action taken. NASA continues to work toward implementing the remaining 26 recommendations, most of which stem from our more recent work.

Next Steps

Consistently securing NASA's IT systems and data while facilitating innovative, user-friendly IT practices will require sustained improvements in NASA's overarching IT governance and security practices. NASA needs to continue its efforts to inculcate solid governance and operations procedures that provide secure, efficient, and cost-effective IT systems for Agency use. Meeting this objective will require increased collaboration among the OCIO, Mission Directorates, and NASA Centers. Additionally, Agency

[13] IG-20-021.

[14] Enterprise computing is the use of IT systems in a centralized structure where the IT department manages technology and users work with standardized products and systems.

leadership needs to demonstrate a concerted and sustained commitment to implement MAP to centralize and consolidate cybersecurity activities and reduce gaps in vulnerability management. Without such sustained improvement, NASA will face continuing challenges in reducing the risk of cyberattacks that expose sensitive information or jeopardize intellectual property.

Moving forward, the OIG will continue to examine NASA's IT governance, security operations, and cybersecurity programs through our audits and investigative work, including the unique challenges presented by COVID-19. For example, an ongoing audit is assessing how well NASA is prepared to identify cybersecurity threats and defend against a major cybersecurity breach. Specifically, we will examine whether NASA's cybersecurity protection strategy is based on appropriate risk factors and whether the Agency's resource allocation is appropriately prioritized. Further, through benchmarking with industry best practices, we will determine how NASA can best assess risk and implement controls focused on sound cybersecurity practices.

Paul K. Martin, NASA Inspector General

Paul K. Martin was confirmed by the United States Senate as NASA Inspector General on Nov. 20, 2009.

Prior to his NASA appointment, Martin served as the Deputy Inspector General at the U.S. Department of Justice, Office of the Inspector General (OIG). In that capacity, he assisted the Inspector General in managing the audit, inspection and investigative activities of the office's 425 employees. From 2001 to 2003, he served as Counselor to the Inspector General, and from 1998 to 2001 he served as Special Counsel to the Inspector General.

Before joining the Department of Justice OIG, Martin spent 13 years at the U.S. Sentencing Commission in a variety of positions, including 6 years as the Commission's Deputy Staff Director. Martin was one of the Sentencing Commission's first employees when the agency was created in 1985, and helped develop the first set of federal sentencing guidelines.

Martin began his professional career as a reporter with The Greenville News, a daily newspaper in Greenville, S.C. He holds a B.A. in Journalism from The Pennsylvania State University and a Juris Doctor from The Georgetown University Law Center.

Martin is married to Rebekah Liu, an attorney working in Washington, D.C. A native of Pittsburgh, Pa., he and his wife have three daughters.

Chairwoman HORN. Thank you, Mr. Martin. Dr. Burley, you're recognized for your testimony.

TESTIMONY OF DR. DIANA L. BURLEY, PH.D.,
VICE PROVOST FOR RESEARCH, AMERICAN UNIVERSITY

Dr. BURLEY. Thank you. Subcommittee Chairwoman Horn, Ranking Member Babin, and distinguished Members of the Committee, thank you for the opportunity to appear before you today. As the Nation continues to navigate the complex and uncertain environment of the global pandemic, it is vital that we engage in a robust discussion on the cybersecurity related challenges and emerging issues for increased telework during this time. At American University we are guided by our strategic plan, Changemakers for a Changing World. AU empowers graduates to navigate, shape, and lead the future of work, and AU researchers are pushing the boundaries of discovery in healthcare, data science, social equity, and security. In my remarks today, which are shaped by a decades-long career leading cybersecurity initiatives, I will highlight how the interplay of these areas supports the development of a holistic strategy to address cybersecurity issues surrounding the exponential growth in telework during this unprecedented time.

Concerns over exposure to COVID–19 have accelerated a mass migration to virtual settings. While teleworking arrangements have existed for years, never before had we seen the range and volume of remote workers or remote working environments. Employees across the spectrum of demographic categories and technical abilities are now working remotely, and engaging with their employers, colleagues, and customers through a digital interface, and on a range of devices. Securing this activity necessitates that we recognize both the technical needs and the environmental factors that shape that behavior. Consider the following. Novice users and novice experiences create vulnerabilities. In the hurried transition to remote work, agencies did not have sufficient time to prepare novice users for the complexity of their newly virtual working environments.

Where overall security is more reliant upon individual decisions made by employees and non-employees alike, even seasoned users who have developed behaviors in accordance with onsite protections face new challenges, and can find themselves less prepared to avoid the vulnerabilities exposed by the remote working environments. Employees are working under duress. COVID–19 continues to drive economic instability, health-related concerns, anxiety, and confusion. Employees are worried about meeting their basic needs, and are less likely to attend to seemingly lower priorities like cybersecurity. Cyber criminals exploit targets of opportunity. The shift in activity provides a larger attack surface, and leads to more opportunities for cyber criminals to use social engineering techniques such as fraud, misdirection, and disinformation to exploit those vulnerabilities.

Users bring their entire selves online. If we use the public health analogy of treating the whole patient, we can strengthen the efficacy of guidance to engage in robust cyber hygiene activities. In public health practice, successful treatment is inextricably linked to the social and environmental conditions of its patients. Today, in

the midst of the COVID–19 pandemic, we must recognize that while basic cyber hygiene practice is relatively doable under normal circumstances, these are not normal times. Our workers are distracted, frightened, and fatigued. This is especially true for the most vulnerable users. As such, strategies to strengthen the cybersecurity of teleworkers must consider the full spectrum of user experiences and address the complex realities of their needs.

The points I have just outlined represent only a snapshot of the benefit of using a holistic approach to reduce the impact of cybersecurity related vulnerabilities. I have long advocated for this type of approach. Now, and with a greater sense of urgency, we must collaboratively develop interventions that address the dynamic interplay between technical and environmental variables that shape the cybersecurity posture across the broad range of teleworkers as they navigate the COVID–19 environment. I look forward to continued engagement with this esteemed Committee to develop concrete strategies that raise awareness of the threat, encourage actions that increase the cybersecurity of the Nation's employees, and protect our most vulnerable citizens. Thank you.

[The prepared statement of Dr. Burley follows:]

TESTIMONY OF

Dr. Diana L. Burley

Vice Provost for Research
Professor, Public Administration and Policy
Professor, Information Technology and Analytics
American University
Washington, DC

BEFORE THE

United States House of Representatives Committee on Science, Space & Technology
Subcommittee on Space and Aeronautics

HEARING ON

Cybersecurity at Nasa:
Ongoing Challenges and Emerging Issues for Increased Telework During Covid-19

September 18, 2020

Online via Video Conferencing

Subcommittee Chairwoman Horn, Ranking member Babin, and distinguished Members of the Committee, thank you for the opportunity to appear before you today. As the nation continues to navigate the complex and uncertain environment of the global pandemic, it is vital that we engage in a robust discussion on the cybersecurity related challenges and emerging issues for increased telework during COVID-19. I appreciate the Committee's commitment to exploring these issues and trust that my remarks today will enhance our collective efforts to safeguard the American people.

My name is Dr. Diana L. Burley. I am vice provost for research at American University (AU) where I am also professor of public administration and policy in the School of Public Affairs and professor of information technology & analytics in the Kogod School of Business. American University researchers develop innovative, impactful, and game-changing solutions to the world's most pressing problems. Guided by our strategic plan, Changemakers for a Changing World, we empower graduates to navigate, shape and lead the future of work. Through the lens of our Changemakers strategy, AU researchers are pushing the boundaries of discovery in health care, data science, social equity and security. In my remarks today, I will highlight how the interplay of these areas support the development of a holistic strategy to address cybersecurity issues surrounding the exponential growth in telework during this unprecedented time.

First, a disclaimer – today I will provide testimony as a private citizen and my views do not represent the official position of American University or any other institution to which I have an affiliation.

My views are shaped by a decades long career leading cybersecurity workforce development initiatives, defining best practices in cybersecurity awareness and education programs, developing strategies to strengthen organizational cybersecurity posture, and informing global cybersecurity policy and practice. I have authored nearly 100 publications on cybersecurity and IT-enabled change. I am a member of the US National Academies of Science, Engineering and Medicine Board on Human-Systems Integration, the Education Council of the Association for Computing Machinery, and an affiliated researcher with the Johns Hopkins University Applied Physics Laboratory. My prior roles have included executive director of the Institute for Information Infrastructure Protection (I3P) and lead program director for the federal Scholarship for Service Cyber Corps program. Notably, the impact of my efforts has been recognized by a range of honors including; SC Magazine Eight Women in IT Security to Watch, a woman of influence by the Executive Women's Forum in Information Security, Risk Management and Privacy, cybersecurity educator of the year, government leader of the year, and a top influencer in information security careers. In short, my experiences across academia, government, and industry provide me with a unique vantage point from which to offer the Committee insight on the subject of this hearing.

Telework During COVID-19

Concerns over exposure to COVID-19 have accelerated a mass migration to virtual settings. While teleworking arrangements have existed for years, never before have we seen the range and volume of remote workers or remote working environments. Employees across the spectrum of demographic categories and technical abilities are now working remotely and engaging with their employers, colleagues and customers through a digital interface and on a range of devices. Securing this activity necessitates that we recognize both the technical needs and the environmental factors that shape user behavior.

Consider the following –

Novice users and novice experiences create vulnerabilities. In the hurried transition to remote work, agencies did not have sufficient time to prepare novice users for the complexities of their newly virtual working environments. Technical capabilities, hardware and software requirements for remote access, were largely the focus of these initial transitional efforts. However, not only does remote work often offer fewer protections, but overall security also is more reliant upon individual decisions by employees and non-employees alike. Even seasoned users, who have developed behaviors in accordance with on-site protections, face new challenges and can find themselves less prepared to avoid the vulnerabilities exposed by their remote working environments.

Employees are working under duress. COVID-19 continues to drive economic instability, health related concerns, anxiety, and confusion. These fears are exacerbated by weather-related disasters, a country divided over racial injustice, and a strained political climate. Employees are worried about meeting their basic needs – safety, food, shelter and health, and are less likely to attend to seemingly less important priorities like cybersecurity.

Cyber criminals exploit targets of opportunity. Everyday more activities move online – people are teleworking, engaging with social networks, learning and shopping. Unfortunately, this shift in activity provides a larger attack surface and leads to more opportunities for cyber criminals. Social engineering methods using fraud, misdirection, and dis-information are all designed to exploit vulnerabilities.

To combat these types of attacks, agencies can adapt cyber awareness campaigns to account for environmental changes and establish strong protocols for robust cyber hygiene practices outside of the workplace. Basic cyber hygiene guidance such as – don't click on links from unknown senders, use strong and unique passwords, set multi-factor authentication, and keep virus protection software up to date, all can make a significant difference.

Users bring their entire selves online. If we use the public health analogy of "treating the whole patient" we can strengthen the efficacy of guidance to engage in robust cyber hygiene activities during COVID-19. In public health practice, successful treatment is inextricably linked to the social and environmental conditions of the patients. Treatment outcomes are the result

of a complex interplay of comorbidities. Today, in the midst of the COVID-19 pandemic, we must recognize that while basic cyber hygiene practice is relatively doable under normal circumstances, these are not normal times. The global pandemic has caused a heightened sense of uncertainty about every facet of life. In the face of this reality, we must be keenly aware that our workers are distracted, frightened, and fatigued. This is especially true for the most vulnerable users. As such, strategies to strengthen the cybersecurity of teleworkers must consider the full spectrum of user experiences and address the complex realities of their needs.

Summary

The points outlined above represent a snapshot of the benefit of using a holistic approach to reduce the impact of cybersecurity related vulnerabilities. I have long advocated for this type of approach. Now, and with a greater sense of urgency, we must collaboratively develop interventions that address the dynamic interplay between technical and environmental variables that shape the true cybersecurity posture across the broad range of teleworkers as they navigate the COVID-19 environment.

At American University, we stand ready to support the nation and the evolution of policy and practice by examining the complex relationship between health care, data science, social equity, and security. I look forward to continued engagement with this esteemed Committee to develop concrete strategies to raise awareness of the threat, encourage actions that increase the cybersecurity of the nation's employees, and protect our most vulnerable citizens. Working together, we can prevent the addition of a cybersecurity crisis to this list of COVID-19 related tragedies facing our nation.

Thank you.

Diana L. Burley, Ph.D.
Professional Biography

Diana L. Burley, Ph.D. is Vice Provost for Research at American University (AU) where she is also Professor of Public Administration and Policy in the School of Public Affairs and Professor of Information Technology & Analytics in the Kogod School of Business. Named one of SC Magazine's Eight Women in IT Security to Watch and the SC Magazine ReBoot awardee for educational leadership in IT security in 2017, Dr. Burley is a cybersecurity expert who regularly advises executives across North America, Asia, Europe and the Middle East on managing cybersecurity risk, assessing the threat environment, and strengthening organizational cybersecurity posture.

She has testified before Congress, is a member of the US National Academies of Science, Engineering and Medicine Board on Human-Systems Integration, the Education Council of the Association for Computing Machinery, and an affiliated researcher with the Johns Hopkins University Applied Physics Laboratory. Prior to AU, Dr. Burley was a professor at George Washington University where she directed the Institute for Information Infrastructure Protection (I3P) – a 26-member national consortium dedicated to strengthening the cyber infrastructure of the United States. She led the Cyber Corps program and managed a multi-million-dollar computer science education and research portfolio for the US National Science Foundation, and has written nearly 100 publications on cybersecurity, information sharing, and IT-enabled change; including her 2014 co-authored book "Enterprise Software Security: A Confluence of Disciplines."

Honors include: 2016 Woman of Influence by the Executive Women's Forum in Information Security, Risk Management and Privacy; the 2014 Cybersecurity Educator of the Year; and a 2014 Top Ten Influencer in information security careers. She is the sole recipient of both educator of the year and government leader of the year awards from the Colloquium for Information Systems Security Education and has been honored by the U.S. Federal CIO Council for her work on developing the federal cyber security workforce.

She holds a BA in Economics from the Catholic University of America; M.S. in Public Management and Policy, M.S. in Organization Science, and Ph.D. in Organization Science and Information Technology from Carnegie Mellon University where she studied as a Woodrow Wilson Foundation Fellow.

Twitter: @dianaburley

Chairwoman HORN. Thank you very much, Dr. Burley. At this point we will begin our first—with our first round of questions, and the Chair recognizes herself for 5 minutes.

Thank you to our witnesses today. It's clear that these are important issues, and there's a lot of things to tackle. And I want to start, Mr. Seaton, with some questions about contractors, as—and cybersecurity contractors, especially given the increased use, and the significant use of contractors within NASA's workforce. So I have a number of questions, I'm going to try and get through as many as we can. Some of them are just yes or no, then we'll get to a few other things.

So what we know, and I mentioned the article today in *The Hill*, is that our systems are—there's a lot of information that hackers are very interested in, and the contractors that NASA works with are integral to our Nation's space agency. So my first question is, are there FAR clauses, Federal Acquisition Regulation clauses, that specifically refer to contractor cybersecurity requirements?

Mr. SEATON. Yes, there are, and we include those in our agency contracts to ensure that our providers follow the cybersecurity requirement.

Chairwoman HORN. OK. So let me follow up on that for a moment, because—so those are NASA cybersecurity requirements? Because we asked earlier this year about associated FAR language, and NASA's response was that there are no FAR requirements, there are no FAR clauses. But to—do those fall under NASA requirements in contracts?

Mr. SEATON. We have a NASA FAR supplement, and to get specifics on what those requirements are included via that, I can certainly take a question for the record to get that.

Chairwoman HORN. OK. Absolutely. And so, when those clauses are included, is it NASA that signs off on the cybersecurity? Are there waivers? What—who signs off on the requirements for cybersecurity, that they've been met?

Mr. SEATON. Well, we have automated tools to be able to ensure that our contractors are complying with the requirements when they're connecting to any NASA system, just as any NASA employee would. So, as was mentioned in the earlier testimony, we've put in place controls, and are continuing to strengthen those controls, to ensure that only authorized devices can connect to our networks and systems.

Chairwoman HORN. OK. And who has oversight of contractor cybersecurity protocols? Is that through your office? Are you able to conduct oversight and audits of cybersecurity practices by contractors?

Mr. SEATON. Ultimately. I am the Acting Information Officer, and so cybersecurity is my responsibility, and so it would be me and my team that ensures compliance with the cybersecurity requirements.

Chairwoman HORN. OK. And do you feel like you have sufficient oversight, and insight, and ability to do that within your authorized—within your authorities?

Mr. SEATON. Yes, I would say that I do believe that, within NASA, I've been given the appropriate authority and support, but I will say that the environment is continuing to change, and it's a

dynamic landscape, as IT is no longer just the computer and the laptop on your desk, but expands to operational technology work. IT is embedded within systems, and so I would say it's challenging with that evolving landscape, and so we continue to mature our processes.

Chairwoman HORN. OK. Thank you. Stepping back to the challenges from this year during COVID–19, I'll have a question for Mr. Martin and Mr. Seaton, and hopefully we'll have time to get to Dr. Burley, about a broader—the memo, Mr. Seaton, that your predecessor published on April 8 warned of increased attempts in cyberattacks, and—especially during COVID–19, and I'm—my first question is—to you, actually, then to Mr. Martin, how has the rate of cyberattacks changed since that memo in April, and what steps has the OCIO taken to respond to those increased attempts?

Mr. SEATON. Well, we have seen an increase in phishing attacks, and a lower level of some other attacks, but honestly, the change to the pandemic operating model is consistent with how NASA has operated in the past. We've supported a mobile workforce, and so have put in place controls and technologies to mitigate against some of these threats, including automated prevention of phishing attacks. Because, when it comes down to it, you and I are the most vulnerable part of our IT security environments, the people, and so we try to put in place automated controls to actually make that easier for our employees, and I've, seen significant improvements in phishing protections over the last 2 years.

Chairwoman HORN. Thank you, and quickly, Mr. Martin, my time is coming to an end, but what is your confidence level in NASA's ability to sufficiently address and increase—the increase in cyber threats as reported by the OCIO?

Mr. MARTIN. Overall I think they're making incremental improvement. They're heading in the right direction, but—and I think there's a real—new realization over the last couple years of the expanse and significance of the challenge, so I think we're very, very cautiously optimistic.

Chairwoman HORN. Wonderful. Thank you very much. I now recognize Ranking Member Babin for 5 minutes of questions.

Mr. BABIN. Thank you, Madam Chair. I think I'm unmuted. Hopefully I am. I want to address this to Chief Information Officer Mr. Seaton. Two weeks ago President Trump signed Space Policy Directive Number Five, which focused on cybersecurity principles for space systems. SPD–5 states, "It is the policy of the United States that executive departments and agencies will foster practices within government space operations, and across the commercial space industry, that protect space assets, and their supporting infrastructure, from cyber threats, and ensure continuity of operations." My question is this. As NASA increases its use of public/private partnerships, how will it ensure that contractors comply with this policy without implementing regulations?

Mr. SEATON. Yeah, thank you for the question. Yeah, so SPD–5, we appreciate the administration and this Congress's focus on space cybersecurity, because that's critically important to us. We're currently in the process of reviewing and analyzing SPD–5, but the good news is we see a lot of consistency with best practices that we are already implementing, and will continue to look to strength-

en our cybersecurity, both within our missions, as well as with our contract partners.

Mr. BABIN. Absolutely. Thank you so much. My next question would be to Inspector General Paul Martin. Your office issued a report on JPL, Jet Propulsion Laboratory's, cybersecurity management last year. JPL, unlike other NASA centers, is managed by a contractor, of course that's Cal Tech. The report highlights the fact that NASA's contract with Cal Tech did not include relevant requirements from NASA IT security policies. And so has the OIG conducted a review of other NASA contractors to determine if their contracts include necessary clauses pertaining to IT security, and if so, how many has your office conducted?

Mr. MARTIN. Thank you, Mr. Babin. We have not conducted a separate audit looking at that specific issue. Although, if I could double back, the concerns we had when NASA entered into a new 5-year contract with Cal Tech, that the contract was absent the significant IT oversight provisions. We have since followed up and found out that JPL has issued, and NASA has accepted, and we've reviewed, and they do meet the criteria that we were concerned about. So the Federal imposed oversight, IT oversight, is going to happen at JPL, so we're pleased for that.

Mr. BABIN. OK. Thank you. And does the OIG conduct compliance audits to determine if contractors are fulfilling their contractual obligations pertaining to information security, and if so, how many has your office conducted there?

Mr. MARTIN. Again, we conduct a significant number of program audits that look at the programs that are run by these contractors, and part of that review includes a detailed dive into the contracts to make sure that the IT security requirements are not only in the contract, but they're actually followed.

Mr. BABIN. Is this a more appropriate role for the NASA CIO or procurement office to conduct, rather than the OIG?

Mr. MARTIN. Well, I think the—certainly the CIO's office and procurement have to ensure at the outset that the appropriate security issues and safeguards are contained in the contract themselves, and ongoing—good contract management would show that you need to ensure that they're being effective. Now, the OIG has limited capacity, like most organizations, and so we're going to try to target the more high risk, high value operations that NASA has to do a deep dive audit.

Mr. BABIN. OK. And then, as this very hearing demonstrates, NASA and the Nation have adopted videoconferencing to adapt to social distancing requirements. Has NASA identified any vulnerabilities with commercial videoconferencing platforms? Are certain videoconference not allowed for NASA use based on technical characteristics or concerns over foreign influence? I would just say—what every one of you have to say. Just a short, concise answer. Appreciate it.

Mr. SEATON. Yes, I'll start with that, and say we have a set of approved tools that have gone through the appropriate security validation, which includes assessing any threats externally to those environments, and, outside of that, other tools are not approved for use within NASA.

Mr. BABIN. OK. And then——

Mr. MARTIN. NASA OIG is using those approved tools.

Mr. BABIN. OK. All right, good. And, Dr. Burley, did you want to add to that at all?

Dr. BURLEY. Most agencies and other organizations have their list of approved tools.

Mr. BABIN. OK. Well, Madam Chair, I've spent all my time, so I will yield back, and I want to thank all the witnesses. We appreciate it very much. Yield back.

Chairwoman HORN. Thank you very much, Ranking Member Babin. And, Mr. Perlmutter, you're recognized for 5 minutes.

Mr. PERLMUTTER. Thank you, Madam Chair, and I think one of the biggest problems with this remote stuff is when somebody like Dr. Babin is walking around with his phone, and I feel like we're in The *Blair Witch Project*, but that's a whole other problem. My questions are for you, Dr. Burley, and Mr. Seaton mentioned the most vulnerable spot for, you know, hacking and cybersecurity is the individual, the person. And when you were testifying, you talked about novice users, you know, not familiar with the equipment or security protocol, employees under duress, worried about their basic needs, and not the more refined things like cybersecurity, you know, that folks are having trouble because they're distracted, frightened, and fatigued, I think were your terms. So what—I mean, it almost feels not that the CIO should be involved, but the Personnel Department is really the—one of the keys here. So what do you see, whether it's NASA, or generally across the agencies, being done to help the individuals kind of get through this very anxious period and maintain cybersecurity?

Dr. BURLEY. Thank you for your question. But—so you're absolutely right in that it needs to be a collaboration between the IT Department and the H.R. (human resources) Department. So, first, every agency has a set of cybersecurity awareness programs that they have in place, and that really guide not only behavior within the organization, within the walls, but also outside. Those awareness programs need to be adapted, recognizing that the employees are working in a different environment, they're working remotely, and they're working around other people. It's not just them. It's also——

Mr. PERLMUTTER. Right.

Dr. BURLEY [continuing]. Family members, and others who are in their environments. And so we have to take a hard look at those awareness programs, and recognize that they need to be adapted based on the current realities of work. And second, yes, absolutely, human resource professionals need to be involved to provide the kind of support to our employees that they need so that they are able to focus on not only doing their work, but doing their work in a secure manner.

Mr. PERLMUTTER. And I guess I hadn't even thought of it, but obviously we should think of it, people are working from home, the kids are in the background, or, you know, whoever might be in the background, so it isn't like you're in the office at NASA headquarters, where everything's pretty safe and secure. So I think, Madam Chair, I'm going to yield back, but I do think this really is cooperation, certainly between the H.R. Department and all of the technology folks. And Mr.—I mean, all three of our speakers

have sort of focused on that, but I—in this pandemic, that's critical, and I yield back.

Chairwoman HORN. Thank you very much, Mr. Perlmutter. Mr. Posey, you're recognized for 5 minutes.

Mr. POSEY. Thank you, Madam Chair, for holding this hearing on this important issue regarding cybersecurity at NASA during COVID–19. Just to recap, in June 2020 NASA's Inspector General stated NASA's high profile and sensitive technology makes the agency an attractive target for computer hackers and other bad actors. And, as stated earlier, during the COVID–19 pandemic, many NASA and contractor employees are teleworking, and possibly making the agency a bigger target. In June 2020 report the Inspector general said it's vital that the agency develop of its information security program to protect the confidentiality, integrity, and availability of its data, systems, and networks. This is not a new problem facing NASA. An assessment by the National Academy of Public Administration (NAPA) concluded back in 2014 that NASA networks are compromised, and that individuals are not being held accountable.

It's not a new concern for us either. I included language in the House-passed NASA authorization bill back in 2015 to address this by requiring a report on how NASA would safeguard its networks and protect against control violations. The Inspector General also made the nine recommendations to NASA, including making sure the risk information security system compliance and data protection capabilities are updated to keep the data secure. And the Inspector General concluded that the threats are increasing, and that it is imperative for NASA to continue its efforts, and strengthen its risk management government practices to safeguard its data from cybersecurity threats.

So, Inspector Martin, first, it was noted that NASA is an attractive target for computer hackers and bad actors. Is China one of those bad actors, and does China present a cybersecurity threat to NASA? And, besides securing its information technology, what steps has NASA done to secure its supply chain from China hackers? And has NASA, or the Inspector General, criminally reported a cybersecurity case involving China to the Department of Justice yet?

Mr. MARTIN. Yes, yes, no. I'm joking. That was a lot of questions. China is one of the foreign entities out there. China's not the sole entity, country, out there that is seeking NASA's very valuable intellectual property. NASA is taking steps, and has been, to secure its intellectual property and its networks from attack both from China and from a series of other countries, and also local hackers. So yes, NASA is—we have conducted a series of criminal investigations, and we work with the FBI (Federal Bureau of Investigation) and counterintelligence officials when we get leads on these issues.

Mr. POSEY. Good, thank you. And Mr. Seaton, with cybersecurity threats increasing, has NASA taken the necessary actions to address the assessment of the National Academy of Public Administration back in 2014, and the nine recommendations identified by the Inspector General, to keep the data security?

Mr. SEATON. Yes. I'm happy to report that we closed out all of the recommendations, there were quite a few, in the NAPA report,

and those have been implemented, and I do think that they improved our security and our practices.

Mr. POSEY. OK, thank you. Dr. Burley, should the National Academy do another study to examine the vulnerabilities that teleworking presents?

Dr. BURLEY. The opportunity for associations and National Academies to do studies gives us an in depth look, and so I would say yes.

Mr. POSEY. Thank you, Madam Chair. I yield back the remainder of my time.

Chairwoman HORN. Thank you, Mr. Posey. The Chair now recognizes Mr. Beyer for 5 minutes.

Mr. BEYER [continuing]. My mute button. Thank you, Madam Chair, very much. Mr. Seaton, thank you very much for joining us today. In your testimony you mentioned that in the course of the pandemic you were able to onboard new employees, new interns, and, amazingly, our office has been able to do the same, wonderful interns and new staff. We've also been able to safely ensure that all staff and interns have House-issued equipment, including laptops and phones. So the—in the OIG report, I was surprised that personally owned devices could connect to internal systems, and that OIG was critical of your not monitoring—enforcing the rules associated with granting access to the NASA networks. So how do you make sure that new employees will be given the proper equipment, and if they're not getting NASA issued equipment, how do we ensure that those personal devices are secured?

Mr. SEATON. Yes, thanks, great question. We actually do require the use of NASA-provided equipment for our new employees and interns, so we do provide them with the tools that they need. Recently, within the last 2 years, it was my office that changed the policy that was referred to earlier, where, yes, previously we did allow personal devices to connect. That is no longer allowed by policy. The only allowance is for a mobile device that has a mobile device management software that we provide that creates a secure container, and a secure connection, back to our e-mail and calendaring systems, if an employee will consent to us managing their personal device with that software. That's the one case where we do allow that.

Where we do have opportunities to continue to strengthen our architecture is implementing the automated controls to ensure that that is what's happening. So network access control, and the pandemic, has actually impacted our implementation there, pushing out that schedule into next year, but we've made significant progress through DHS, the CDM (Continuous Diagnostics and Mitigation) Program, to know what's on our network, and who's on our network, and have a little bit more to do there.

Mr. BEYER. Good, good. Thank you. That's encouraging to know, because I'm sure the stuff you have is much more important than the thing that's on my network. Mr. Martin, you talked about the malicious intrusions in the NASA systems, you know, unauthorized access to Deep Space Network. Other than the personally identifiable information, what are they after, and how much of this is China, Russia, the other nations that are interested in space, and will this affect, or could this affect, our lunar missions or Mars mis-

sion, James Webb, and some of the really big important things that NASA's doing?

Mr. MARTIN. Thank you, Congressman Beyer. NASA has vast troves of important intellectual capital that it has spent decades amassing, and so I think folks are—country actors are after that information, the innovations that NASA's so famous for around the world. There's everything from PII, there's contractual data on the systems, so there's just a vast and wide array. And, again, we've had—NASA, unfortunately, has been under attack from both domestic and foreign cyber criminals, and so it is just an ongoing, incredibly difficult issue to keep NASA's defenses up.

Mr. BEYER. OK, thank you very much. And, Professor Burley, you know one of the challenges NASA has, obviously is that they're so decentralized. So many of us have NASA facilities near or close, and so a one size fits all is always going to be difficult. Are there other examples of systems, especially Federal systems, that are similarly decentralized that have been able to effectively secure their IT systems? Are there anybody for NASA to imitate or emulate?

Dr. BURLEY. I think that the CIO from NASA would know better, but there are many different decentralized systems, both within the Federal Government and outside, that could be used as a guide to at least begin to think about best practices and other strategies for securing the networks.

Mr. BEYER. Let me pivot to Mr. Seaton, then, quickly, because I know, like, Department of Commerce had 13 different CIOs. Do you have the same challenge within NASA?

Mr. SEATON. Yeah. So there's one CIO, but there are center CIOs. They all report to me. We have a single IT strategy, and, for almost a decade now, we've been working to integrate and operate as a cohesive unit, acknowledging that there are some uniquenesses at our centers, but implementing consistent policies, and moving toward enterprise services and contracts. So I think we are moving in the enterprise direction very significantly.

Mr. BEYER. Thank you very much. And, Madam Chair, I yield back.

Chairwoman HORN. Thank you very much, Mr. Beyer. Mr. Garcia, you're recognized for 5 minutes.

Mr. GARCIA. Thank you, Madam Chairwoman, appreciate it, and appreciate the testimony and the witnesses today. Very exciting times for NASA, and also very challenging, with very unique dynamics in play here. I guess I've got a few questions, and probably directed to all of you, Mr. Seaton, Mr. Martin, and Dr. Burley. I come from a company where I was a program director for a large air breather program, and it was both classified and unclassified elements to it. One of the big challenges that we had as a large prime was that the classified elements fell under NISPOM (National Industrial Security Program Operating Manual) requirements, which I think were effectively what Chairwoman Horn was asking about on the classified side, as far as our compliance and requirements. Those requirements led to onerous costs to suppliers, and to the lower level supply chain folks.

What is NASA doing, I guess, to make sure that the small businesses that are a critical element of your supply chain aren't nec-

essarily getting overwhelmed with either cybersecurity requirements, or cybersecurity development work, software development work, and therefore almost being dissuaded from entering into this industry, into this support chain? Are we able to provide GFI, or government furnished IP (Internet Protocol) to make sure and flow down to the lower level suppliers to make sure that they're baking in some of these cybersecurity elements into their respective programs, or how do we communicate, I guess, with those lower tier supply chain folks? I guess, Mr. Seaton, we can start with you.

Mr. SEATON. Sure. I will say that is a challenge. Making sure that all of our suppliers and providers appreciate the significance of cybersecurity, and are building that into the solutions they deliver, is a requirement of doing business today, right, today with supply chain risk management. Just in August Section 889 was enacted, that requires us to certify that anybody we're doing business with complies with supply chain restrictions that are Federal-wide. So we're working with our providers and suppliers to make sure they understand, and that they build that into their practices.

Mr. GARCIA. Yeah, I just, you know, we ought to just make sure we're balancing the risk mitigation efforts, which are absolutely critical and essential. We have to do it with the cost elements, and the, you know, just making sure that we're not driving some of these key suppliers out of business, or out of our industry, or out of your business, right? I know that's a delicate balancing act as well.

Mr. SEATON. True. The cost of having a compromise is significant too, though, so you're right, it is a balancing act, and we'll continue to try to work.

Mr. GARCIA. Are the primes, or tier one suppliers, actively looking to package up programs or software, you know, programs to download to the lower level suppliers, or is it sort of ad hoc, depending on what the threat is, and what the threat mitigation measure is?

Mr. SEATON. Yeah. Unfortunately, I really can't speak to the individual practices of the companies and suppliers.

Mr. GARCIA. OK. And then I guess just characterizing classified versus unclassified, are you able to speak to what percentage of your networks are on unclassified networks, and is one of the sides lagging the other? In other words, do you see, you know, more threats on the classified side, or fewer threats, but maybe more, you know, more critical impact to those networks? Or how would you characterize the deltas there between unclassed versus the high side?

Mr. SEATON. Yes, and my office is responsible for the unclassified side. We work with our Office of Protective Services on the classified side. I can't really speak in this forum to kind of the division there, but I will say that oftentimes compromises on the unclassified side can be used to propagate to other systems that—and so that's a concern, even on the unclassified side.

Mr. GARCIA. OK, great. Yeah. And, Mr. Martin or Dr. Burley, I don't know if you guys care to comment on either of those topics there.

Mr. MARTIN. We have little or no work on the classified side at NASA.

Mr. GARCIA. OK. That's good to know. OK. So I would just, you know, we hosted a small business summit with Kevin McCarthy as well, and with the NASA Administrator Bridenstine a couple of weeks ago. The cost of entry into the supply chain for all space programs is pretty high for some of these small suppliers, so I would just end with let's try to enable them, let's make sure we're giving them the tools to be successful and be able to defend not only their networks but yours, obviously, as your suppliers as we navigate this challenge, and hopefully look to synergize lessons learned and download those through contract requirement flow-down documents accordingly. So, really appreciate your guys' time, and good luck with the upcoming launches as well, guys, thank you. I yield back.

Chairwoman HORN. Thank you, Mr. Garcia. And now, for the honorary Member of our Subcommittee, who is reliable and with us, Mr. Weber, you're recognized for 5 minutes. If we can get you unmuted. There you go.

Mr. WEBER. There we go. There's a lot of people who want to mute me, but nonetheless, thank you for that, Chairwoman, and I appreciate the opportunity of being here. You actually asked a question to Mr. Seaton earlier, I think, about how many intrusion attempts per month that NASA identified last year, and I want to kind of follow up on that by saying how does that compare, Mr. Seaton, to the intrusion attempts per month this year during COVID? Are you making a distinction there?

Mr. SEATON. Yeah, so—not that direct comparison, and we see fluctuations based on our insight, and that insight, as I mentioned, is increasing, so sometimes that is the cause for a higher number. But we have seen an increase in phishing attacks and malware attacks at various times throughout the pandemic. That hasn't been steady, it's been fluctuating.

Mr. WEBER. Any idea or guess, 10 percent, 20 percent, five percent, increase?

Mr. SEATON. At one point, over a given period of time, we saw a doubling of phishing attacks, but, again, there have been other weeks where it's been lower. So I do think, because of the pandemic, people are looking for the opportunity to attack, and will continue to.

Mr. WEBER. Well, there's been a lot of discussion about, you know, having personal devices, and being at home, and those kinds of security firewalls, if you will. And if it's sensitive information, I know you said you worked with the FBI and some of their forces, or task force, I forget the terminology you used, that sensitive information, if you could get it to us, it would be interesting for us to have, get it to my staff. And I want to follow up in your discussion with Mr. Garcia. You all talked about, well, before I do that, let me go to Mr. Martin really quick.

Mr. Martin, understanding that this hearing is supposed to be merely focused on cyber threats during COVID, since you're here with us, I thought it'd be appropriate to discuss some of the things we've been talking about with China, for example. Intellectual property threats to the aerospace U.S. supply chain, you all talked about it a little bit, I think, with Mr. Garcia. During this week's Air Force Association Aerospace and Cyber Conference it was revealed that a longtime DOD (Department of Defense) and NASA

launch provider, UL Lab, proactively, I don't know if you're familiar with this, proactively identified and cut ties with the supplier that was a security risk due to Chinese ownership. Were you aware of that, Mr. Martin?

Mr. MARTIN. I was not, Congressman.

Mr. WEBER. OK. Well, in comments earlier, I think I'll go back to Mr. Seaton, with his exchange with Garcia, he said he couldn't speak to suppliers or speak for the suppliers. Is that what you were saying to Mr. Garcia?

Mr. SEATON. I said that I could not speak to how they were structuring their business operations to meet the Federal requirements.

Mr. WEBER. Shouldn't that be something that we're looking at? I mean, I don't mean to sound too skeptical, but shouldn't NASA and actually, all of our U.S. space and defense companies should be taking a proactive posture to know exactly what safeguards are in place for a supply chain?

Mr. SEATON. Totally agree. So how they go about doing it, is what I'm saying, that we're not in their business operations. Validating that they are complying with the requirements is something that we've been doing for years with our supply chain risk management efforts, ensuring the things that we buy are free of risks through coordination with the FBI, and now making sure that, even within their organizations, they do not have IT equipment provided by prohibited providers. So, yes, we are actively involved in ensuring that level of compliance.

Mr. WEBER. Well, you say how they go about it you're not necessarily involved in, but shouldn't there be some level of protocol, for lack of a better term, some threshold, some safeguard, they have to meet minimum safeguards, and somebody has to be looking over their shoulder in that regard? Is that fair to say?

Mr. SEATON. Yeah. Again, compliance with our cybersecurity requirements is absolutely critical, and that is our responsibility. How they—their business practices is what I'm saying that we are not getting in the middle of.

Mr. WEBER. Would you say that, in this particular instance, where that supplier was identified, that it would be worthwhile to go back and see exactly how that happened, how that supplier got the proverbial camel's nose under the tent?

Mr. SEATON. I think it's in the Federal Government's best interest to understand where vulnerabilities emanate from, so, certainly.

Mr. WEBER. Whose responsibility is that?

Mr. SEATON. I think it's a shared responsibility.

Mr. WEBER. Between who?

Mr. SEATON. Between the Federal agencies that are responsible for our cybersecurity policy, as well as an agency that would be interacting with a specific provider.

Mr. WEBER. Is that something you could follow up with our office on, and tell us who those agencies are, and who has responsibility for that agency? And I'm talking about addressing this particular instance, and how it was discovered, and how we got there, and what steps are going to be taken to prevent similar occurrences. Can you follow up with us on that?

Mr. SEATON. Certainly. We'll take that as a question for the record, yes.

Mr. WEBER. OK. Well, I appreciate that. Madam Chair, I yield back.

Chairwoman HORN. Thank you very much, Mr. Weber. Appreciate your questions, and, as always, your participating in the Subcommittee. I think—I have a few more questions I want to follow up with, and we'll have an opportunity for the Members to do another round of questions, if everyone is available to stay, since we're still—we still have time.

I have—I want to follow up on a couple of things, going back to some of the earlier questions about—one about the unauthorized devices, or personal devices, and then I do want to follow up Mr.—on Mr. Weber's line of questions a little bit more. Mr. Martin, the August 2020 IG report on unauthorized devices, which was of course just this year, on NASA's network cites CIO's office, saying that there—currently no authoritative way to obtain the number of partner-owned IT devices. And I know, Mr. Seaton, you mentioned that you're not allowing that anymore, but it seems that that's still happening. So, Mr. Martin, I'm wondering what the risks are of not being able to identify, and why that may be the case, from your perspective, in this report? And then, Mr. Seaton, I want to follow up with you about what NASA's doing to improve its understanding and insight into those devices. So, Mr. Martin, if you want to start with that?

Mr. MARTIN. Sure. If I could say at the outset, NASA—as I said in my oral remarks, NASA has been searching for that balance between user flexibility and system security, and during the 10 years that I've been at NASA, it has somewhat wildly lurched from those extremes. I remember early on, a number of years ago, where they had a BYOD policy, which was a bring your own device policy, and that's how sort of forward leaning NASA was about allowing employees, and even contractors, to use their personal devices.

Now, in the last couple years, NASA has taken a much more measured approach, and have focused recently, but there are still gaps that remain in the security of these mobile devices. So, as you indicated, in the report that we issued just last month, they have implemented software, but they haven't fully implemented the controls to remove or block devices from NASA systems that shouldn't be on that NASA system. And they're also not adequately monitoring the business rules for granting access with a personal device to NASA's network. They're not enforcing consistently the business need for that, and they're also not ensuring that each of the mobile devices, the personal mobile devices that connect to the system, don't violate supply chain rules.

Chairwoman HORN. OK. Thank you very much, Mr. Martin. Mr. Seaton, I know you've taken steps in that direction. Can you speak to, I know there's been a delay, but the—what you're doing, what NASA's doing, to address these holes? It sounds like you've made progress, but what are—what is NASA and what is the CIO doing to address these other outstanding issues?

Mr. SEATON. Sure. Actually, as an agency, I believe—I think we have been a leader in implementing the—DHS's continuous diagnostic and mitigation program, where CDM phase one identified

what was on the network, and so we had tools in place to automatically detect what's on the network. Phase two, which we are in the middle of implementing right now, is controlling who is on the network, and that gets to the network access control element that Mr. Martin spoke of. And, again, I think in the—we will in the coming year, be able to enable those controls to be able to have a technology-based way to enforce the policy that has been issued by my office.

Chairwoman HORN. Thank you very much. And, just following up on a couple of Mr. Weber's questions, in terms of the insight, getting back to the—some of the first questions about contractor requirements, and how we control for suppliers and information, there's a balance between overly burdensome requirements and the opportunity for bad actors to influence or to gain access, and I'm wondering, Mr. Martin, what you see as potential authorities that NASA may need to be able to have additional insight, or control, or contracting provisions to ensure that there's compliance all the way up and down the supply chain. Is it with the primes, or are there other provisions that may be needed?

Mr. MARTIN. I'm actually going to answer that question by focusing in house on NASA. We have commented for the last—we did an audit in 2014, and a follow-up in 2017, and one of our concerns was just how NASA is structured, where—is Jeff, or whoever's sitting in the CIO's position, doesn't have full insight into all of NASA's systems. In fact, doesn't have full control over the IT spend, and enforcing the IT security requirements, particularly in mission systems and center systems. Jeff and his colleagues have full control over what's known as the institutional systems, but they make up about 25 or 30 percent of NASA's overall budget, so the lack of insight and oversight wielding the stick that controls the money on the end of it is a real governance issue.

Chairwoman HORN. Thank you very much, Mr. Martin. And, Mr. Seaton, do you want to speak to that quickly? It sounds like you need—to be able to do that you need additional authorities, or insight and oversight.

Mr. SEATON. Actually, I think that that has been changing. I sit on the Agency Program Management Council, the Mission Support Council, and the Acquisition Strategy Council as a full member, so I have insight into major agency decisions, and the administration fully supports the programs and plans that we're putting in place, and then the collaboration with the missions to ensure their systems are secure, where we now have much more widespread, effective, consistent approaches to authorities to operate. And I've been working with the Council of Deputies within NASA to ensure that we have the appropriate mission leadership, senior executives, designated as authorizing officials for those mission systems. So I do think we're making significant progress, excuse me.

Chairwoman HORN. Thank you very much, Mr. Seaton. Mr. Babin, you're recognized for 5 minutes. Do you have more questions?

Mr. BABIN. Yes. Can you hear me? OK, thank you. I do have some more questions. I wanted to address this to all the witnesses, if possible. How many intrusion attempts per month did NASA identify last year? How does that compare to the intrusion at-

tempts per month this year, during COVID? And if this information is sensitive, please provide a response to the staff after the hearing concludes.

Mr. SEATON. Yeah. If I could take the specifics as a question for the record, but I can speak in more general terms. As I mentioned before, I think the measurement of intrusions continues to fluctuate based on our insight into the network, and that has increased. So, in some cases, where we see an increase in intrusions, it's because we're seeing more of what's happening, and we're to the point now we've got, I think, a pretty solid visibility into our network today. But then a comparison of specific month by month, we'll have to take that and get back to you.

Mr. BABIN. OK. All right. Thank you. I think I will yield back for Madam Chair.

Chairwoman HORN. Thank you very much, Mr. Babin. Mr. Beyer, you're recognized.

Mr. BEYER. Madam Chair, I have no more questions. I keep learning, but I yield back.

Chairwoman HORN. Excellent. Thank you. Mr. Garcia?

Mr. GARCIA. Thank you, Madam Chair. Just a real quick question. You know, the old adage that the best defense is a good offense is kind of appropriate here. Mr. Seaton, are you happy with the support that you're getting form other government agencies? In terms of the development at a national level we develop offensive cyber capabilities. That informs your defensive cyber techniques and vulnerabilities. Are you comfortable and satisfied with the communications, I'll just say, to other government agencies that should be informing you as to where the state-of-the-art is going, in terms of offensive cyber capabilities which may, you know, be in the hands of the bad guys, and be within our own domestic networks? If not, where can we help to maybe, you know, improve your ability to leverage the developments of other equities outside of NASA?

Mr. SEATON. Yeah, I think the administration's been very supportive of our need to continue with the appropriate focus on cybersecurity, and I think that NASA has effective relationships with our counterparts that can provide us counterintelligence information, as well as, you know, best practices on cybersecurity, the Federal CIO Council, the CIOs across the Federal agencies engaging to share information is another effective mechanism for that information sharing.

Mr. GARCIA. OK. So the historical, I'll call it just historical evidence over the last call it two years, though, have there been any surprises, I guess, from the threats where it was a completely unknown rider coming in through an unknown technique or vulnerability that really hadn't been discussed? I know that there's sensitivities around how much you can say here, but, you know, any sort of unknown riders that just completely caught you off guard that we ultimately found out another equity throughout the government maybe had been aware of?

Mr. SEATON. Yeah. I think, because of the dynamic landscape, we're going to face surprises. We want to minimize those, right?

Mr. GARCIA. Sure, sure. Yeah.

Mr. SEATON. But I will say that there have been times when other agencies have observed activity, and contacted NASA, and then we would partner on that. So, again, I think the communication mechanism—mechanisms are there.

Mr. GARCIA. That's good. Well, that's encouraging to hear. A lot of these lessons learned have been learned, you know, several times before, so we can avoid duplication of lessons learned, especially in this cyber domain. That's a huge benefit to you guys.

Mr. SEATON. Certainly.

Mr. GARCIA. Thank you. I yield back, Madam Chair.

Chairwoman HORN. Thank you very much, Mr. Garcia, and thank you to all of our Members for their thoughtful, intentional questions, and to all of our witnesses. It's clear that these are critically important issues that NASA is facing, as well as some important lessons learned during COVID–19, as Dr. Burley stated, that these are not normal times, so our strategies during COVID–19 are important, but also inform cybersecurity more broadly. And I think that it sounds as—that NASA is making progress, but that, as a—as the authorizing Committee, we want to ensure that you have sufficient authorities and funding capabilities to have strong cybersecurity practices and protocol in place, and we continue to move forward with the recommendations and implementations from the GAO, and other strategies that ensure not just the 25 percent that you have authority—direct authority over, but the contractors, especially given some of the things that we have seen.

So, unless any of our Members have further questions, we'll bring this hearing to a close today. I want to thank again the witnesses for your testimony, and for your time, and for what you do. The record will remain open for 2 weeks for additional statements from the Members, and additional questions of the Committee, or that the Committee or Members may ask of the witnesses. Thank you all again for your time. The witnesses are excused, and the hearing is now adjourned. Thanks, everybody.

[Whereupon, at 12:20 p.m., the Subcommittee was adjourned.]

Appendix

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Jeff Seaton

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON SPACE AND AERONAUTICS

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

Questions for the Record to:

Mr. Seaton

Submitted by Chairwoman Horn

1. **In response to my question during the hearing, you stated that you could provide more information on cybersecurity requirements in NASA contracts. Please provide all contractor cybersecurity requirements included in the NASA Federal Acquisition Regulations supplement.**

NASA Response: NASA's Office of the Chief Information Officer (OCIO) works with the information system owners and contracting officers to ensure that contract requirements are enforced.

Specifically, the clause at NASA Federal Acquisition Regulation (FAR) Supplement (NFS) 1852.204-76, *Security Requirements for Unclassified Information Technology Resources,* is NASA's primary cybersecurity clause. NASA uses this clause in all solicitations and awards when contract performance requires the contractor/vendors to either have physical or electronic access to NASA's computer systems, networks, or information technology (IT) infrastructure, or to use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

The -76 clause takes a multifaceted approach to enhancing a contract's cybersecurity posture. First, the clause requires the contractor to develop and submit two plans to NASA: an IT Security Plan, and an IT Security Management Plan. The Security Plan is focused on securing IT systems and is required to demonstrate that contractor's compliance with all relevant Federal laws, including the 2014 Federal Information Security Modernization Act (P.L. 113-283; "FISMA"). The Management Plan is required to describe the processes and procedures that the contractor will employ to ensure appropriate security of IT resources that are developed, processed, or used under the contract.

Second, the -76 clause contains a requirement that all contractor personnel requiring physical or logical access to NASA IT resources must complete NASA's annual IT Security Awareness training.

Third, the clause provides NASA explicit authority to access the contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract for the purpose of performing an IT inspection (to include vulnerability testing), investigation, and audit.

Finally, the clause requires that NASA compile, and attach to the contract, an Applicable Documents List in which NASA specifies those documents that contain additional cybersecurity requirements and policies tailored to that specific contract.

2. **You stated in response to my question at the hearing that NASA employs automated tools to ensure compliance with the cybersecurity requirements of the Federal Acquisition Regulations (FAR) and the NASA FAR supplement. What information do the automated tools look for or check? To what extent is the use of such tools in ensuring contractor compliance a standard practice throughout the federal government?**

NASA Response: NASA has implemented the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program tools. Through the CDM program and enabling tools, NASA has implemented a continuous monitoring capability to monitor for software vulnerabilities and security configuration standard compliance status on Agency systems. These tools report findings to information system owners and NASA's Security Operations Center and are monitored through the system lifecycle. This data is also fed up to the DHS Federal CDM Dashboard.

3. **How do NASA cybersecurity requirements for contractors flow down to subcontractors and supply chain providers that support implementation of those contracts?**

NASA Response: NASA requires our prime contractors to meet the requirements of their contractual agreements with NASA, including meeting all cybersecurity provisions included in their contractual agreements with NASA as well as any Federal laws applicable to doing business with the Federal Government. It is important to remember that NASA does not have direct relationships with subcontractors or specific insight into a prime's managerial relationship with its subcontractors. Instead, our contractual relationship is with a prime contractor, and therefore, we expect Agency primes to manage their subcontractors, and to ensure that all policies, provisions, and clauses in any prime contract are shared with their subcontractors and enforced.

4. **What cybersecurity and information security requirements does NASA impose in contracts when procuring space operations as a commercial service—for example, through the Earth Science Commercial Smallsat Data Acquisition Program, the Commercial Crew Program, and the Commercial Lunar Payload Services initiative—and what is the formal role of the Office of the Chief Information Officer in developing these requirements and ensuring they are met?**

NASA Response: In addition to utilizing the NFS clause and tailored Applicable Documents List described in response to Question 1, NASA, with input from OCIO, adds additional cybersecurity requirements tailored to each of its contracts. Procuring space operations as a commercial service does not necessarily, on its own, reduce the volume or materially change the type of cybersecurity requirements within a contract, as NASA must ensure that its missions are fully protected from threats at all phases of performance, regardless of whether NASA is performing the mission or has hired a commercial partner to perform it in conjunction with, or on behalf of, NASA.

5. **In response to one of my questions during the hearing, Mr. Martin stated that the Office of the Chief Information Officer (OCIO) does not have full insight into all of NASA's information technology (IT) systems (and associated spending), specifically mission and Center IT infrastructure, and that "the lack of insight and oversight—wielding the stick that controls the money on the end of it—is a real governance issue." However, in answering my question, you stated that you think that you are seeing "significant progress" in this area due to changes you noted, which include placement of the CIO on various councils and collaboration with missions. What indicators or evidence of progress are you**

seeing in your insight and oversight of mission and Center IT systems and spending as a result of the actions you mentioned?

NASA Response: Over the last several years, NASA has established a new governance structure that gives the NASA Chief Information Officer (CIO) greater visibility and authority within the Agency, including:

- Increasing the responsibility, accountability, and authority of the NASA CIO in order to drive efficiencies and cost-savings through the acquisition, deployment, and management of IT across NASA, while also ensuring that the CIO reports directly to the Administrator;
- Establishing IT acquisition process changes, ensuring that, in partnership with the Office of Procurement, the NASA CIO approves IT acquisition strategies and IT acquisition plans, as well as leverages strategic sourcing; and
- Using a Government-wide acquisition vehicle called Solutions for Enterprise-Wide Procurement (SEWP) to help NASA manage a suite of Government-wide IT products to meet the requirements of FITARA.

Additionally, NASA has aligned IT and mission strategy in order to achieve goals and measure performance while ensuring stakeholders are informed including:

- Strengthening the Agency's ability to align IT resources with Agency missions, goals, programmatic priorities, and statutory requirements;
- Clarifying the scope of the Agency CIO's role with respect to program IT and mission IT decisions, as well as allowing the CIO to participate in major Agency decision making processes for Agency missions, including the Agency Program Management Council;
- Holding the CIO accountable for Agency IT cost, schedule, and performance through a new portfolio review process including new authority and greater visibility into the overall budget planning cycle, allowing the CIO to spot IT resource problems at a mission level earlier on;
- Increasing transparency of IT resources across the entire Agency; and
- Ensuring that the IT security policies and procedures are implemented throughout the NASA enterprise, including at our Centers. As mentioned at the hearing, several years ago, NASA realigned the reporting structure so that the NASA CIO has direct authority and oversight over the Center CIOs.

Over the last several years, OCIO, and in particular acting CIO Jeff Seaton, and the NASA Senior Agency IT Security Officer, Michael Witt, have made a concentrated effort to reach out to the Mission Directorates to better understand their IT needs and their concerns about IT's impact on their missions as well as how to better integrate cybersecurity into the mission project management lifecycle. For example, in order to address the unique cyber risks and challenges posed by human spaceflight, and in particular by NASA's Artemis Program, OCIO has partnered with the Human Exploration and Operations Mission Directorate (HEOMD) and its Advanced Exploration Systems Division at NASA Headquarters. A senior OCIO staff member is engaged in program planning and leadership meetings, providing immediate OCIO input on relevant cybersecurity and programmatic matters. This partnership allows OCIO to better understand HEOMD's programs, processes, and mission requirements while helping HEOMD leadership identify and resolve any cybersecurity gaps by evaluating cybersecurity requirements, ensuring an integrated approach to addressing cybersecurity risks, and making certain that cybersecurity considerations are included at the outset of this groundbreaking work. In addition to its partnership with

HEOMD, OCIO continues to proactively work with other NASA projects and missions to strengthen mission cybersecurity and to support emerging IT requirements.

Additionally, as noted by Mr. Seaton at the hearing, as the acting CIO, he has a healthy, collaborative relationship with the Center CIOs and their leadership teams. In parallel, NASA is continuing to centralize our IT services in an Agency-wide enterprise delivery model, with full program oversight and authority over services deployed across NASA Centers. In doing so, OCIO is implementing and delivering CDM capabilities at the enterprise-level, providing enterprise visibility into all NASA hardware assets and information systems.

6. **In April 2020, the Government Accountability Office (GAO) wrote that one of the highest-priority open recommendations for NASA is that the agency "should establish a process for conducting an organization-wide cybersecurity risk assessment." What is the status of NASA's effort to meet that recommendation and other GAO recommendations to fully establish its agency-wide approach to managing cybersecurity risk—including defining a strategy, roles and responsibilities, and establishing a process for organization-wide risk assessments—and what remains to be done?**

NASA Response: NASA is appreciative of the GAO's recommendation, with which we concurred. NASA is continuing to work with other Federal cybersecurity partners to meet this recommendation in a thoughtful and expeditious manner. NASA OCIO has also hired a Chief Cybersecurity Risk Officer responsible for the NASA Cyber Risk Management Strategy.

7. **What is NASA's role in the National Security Council's Space Cybersecurity Interagency Working Group, and how does involvement in the working group benefit NASA?**

NASA Response: NASA would defer questions regarding the activities of a National-Security-Council-led (NSC) interagency working group to the NSC.

8. **To what extent was NASA involved in the development of Space Policy Directive 5, "Cybersecurity Principles for Space Systems," released by the White House on September 4, and how, specifically, will NASA implement the policy?**

NASA Response: NASA participated in the interagency review of Space Policy Directive (SPD) 5. In keeping with SPD-5 guidance as well as the FISMA requirement, NASA leverages a risk-based, cybersecurity-informed approach to our mission systems' development and operations. NASA implements the cybersecurity risk management framework and associated guidance on security controls provided by the National Institute of Standards and Technology (NIST). Further, NASA has issued a new engineering technical standard for the protection of space systems which supports the intent of SPD-5. Therefore, there is a lot of consistency between SPD-5 and the best cybersecurity practices NASA has already implemented within the Agency, and we will continue to strengthen our cybersecurity processes both within our missions as well as with our contract partners.

9. **Why does NASA not know, as reported by the OIG in its August 2020 "Audit of NASA's Policy and Practices Regarding the Use of Non-Agency Information Technology Devices," how many partner-owned devices are accessing NASA networks?**

NASA Response: NASA agreed with the Office of Inspector General (OIG) recommendation and was already working to automate the inventory and control of network access as part of our efforts to implement the DHS CDM Program. NASA implemented CDM Phase 2, which included identifying "who" is on NASA's network along with privilege access. CDM Phase 3, which focuses on "network security management" is being worked with DHS as part of the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) contract. OCIO is currently on schedule with DHS in its deployment of technologies to monitor unauthorized IT device connections designed to remove or block these devices from accessing NASA's networks and systems.

10. **In responding to a question by Mr. Beyer during the hearing, you stated that the pandemic has affected NASA's implementation of improved procedures around network access controls, including delaying the schedule to next year. How has the pandemic delayed the implementation, what actions are required to complete implementation, and what is your current target date for completing implementation?**

NASA Response: Today, OCIO's job is even more challenging with the vast majority of NASA's workforce – both civil servants and contractors – teleworking from remote locations across the country due to the pandemic. Thus, the NASA CIO has shifted priorities to address the need to support a mostly remote workforce. We anticipate completing the implementation of Network Access Control in late FY 2021.

11. **NASA reported a total of 317 cybersecurity incidents in its Fiscal Year (FY) 2018 Federal Information Security Modernization Act (FISMA) submission to the Office of Management and Budget (OMB), a significant decrease from 1,847 reported in FY2017. However, the FY2019 number rose to 1,469. Please explain why NASA saw a large decrease from FY2017 to FY2018, and then a large increase from FY2018 to FY2019, in the total number of reported cybersecurity incidents, and why the FY2019 increase is predominately reported in the "improper usage" category of incidents.**

NASA Response: NASA follows guidance from DHS' Cybersecurity & Infrastructure Agency (CISA) – formerly known as US-CERT— about what an "incident" is and what should be included in the statistics reported to that agency. However, the definition has changed over the years.

In FY 2017, NASA was required to include lost and stolen devices as incidents – incidents which were categorized as unauthorized access. Therefore, the decrease in NASA-reported incidents between FY 2017 and FY 2018 can largely be explained by a decision to exclude the reporting of lost or stolen device incidents to CISA from the total incident count in FY 2018.

The increase in the reported number of incidents between FY 2018 and FY 2019 can largely be attributed to changes in NASA's implementation of Data Loss Prevention (DLP). When DLP was implemented at NASA in FY 2019, the automated tool identified and flagged Sensitive But Unclassified (SBU) material in emails. Agency policy requires that SBU material be encrypted when sharing by email within the Agency. Therefore, any SBU material that was not appropriately encrypted when transmitted, was identified by DLP and categorized as an unauthorized access incident and thus reported to DHS/CISA as an incident. NASA OCIO later decided to categorize these DLP-identified incidents as improper use, as opposed to unauthorized access, which meant they were no longer reported as "incidents" to DHS/CISA.

12. Your prepared testimony notes that NASA received the highest rating ("Managing Risk," the highest on a three-level scale) on the Fiscal Year (FY) 2019 Federal Information Security Modernization Act (FISMA) self-assessment. On a different scale, however, the Office of Inspector General (OIG) independent FY2019 FISMA assessment rated NASA as Level 2 ("Defined Risk") of 5 for the fourth year in a row. How should Congress consider these assessments, given what appear to be conflicting conclusions?

NASA Response: As noted in our response to Question 5, over the last several years, NASA has made major progress in improving our IT management through key governance changes that have greatly empowered the CIO's role within the Agency and also by implementing new technologies to improve the protection and management of our network. We are also doing a better job of educating our employees about their role in both missions. The FISMA OCIO metrics measure the efficacy of NASA's cybersecurity capabilities and tools, while the NASA OIG-developed metrics evaluate the maturity of the NASA OCIO's business processes and policies. While NASA is "managing risk" in terms of the fundamental cyber capabilities we provide, we recognize that there is always more work to be done – our business never stops changing. Therefore, protecting and evolving the NASA IT infrastructure continues to be a top Agency priority.

13. Of NASA's ten most expensive information technology (IT) investments, four are categorized as "non-major" in the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) framework. Why are these four expensive investments—which include high-profile and high-priority programs for the agency, such as the Orion Crew Vehicle program and the International Space Station—not designated as "major" and receiving more thorough oversight and attention?

NASA Response: NASA follows the Office of Management and Budget (OMB) Circular A-11 Preparation, Submission, and Execution of the Budget and the A-11-referenced OMB Capital Planning Guidance. In alignment with the Capital Planning Guidance, as part of Capital Planning and Investment Control (CPIC), the NASA CIO works in partnership with Agency leaders via the IT Council to evaluate IT investments and determine which IT investments meet the criteria to be a NASA major investment to be reported to the IT Dashboard.

14. Some of NASA's existing information technology (IT) infrastructure is aging, which can leave it vulnerable to cyber-attacks. How does NASA's aging infrastructure affect NASA's cybersecurity vulnerabilities, and what NASA's plans are to update its aging IT infrastructure? What are the biggest barriers or challenges to modernizing the agency's hardware and other aging IT infrastructure?

NASA Response: NASA is appreciative of the funding that Congress continues to appropriate for NASA OCIO and the Agency's IT infrastructure. However, budgetary delays also drive delays in NASA's ability to implement new technology initiatives, which can delay our modernization curve and increase NASA's cyber risk posture. Additionally, NASA is concerned that appropriations have consistently fallen short of the Agency's requested budget for the Safety Security and Mission Services account. This funding supports modernizing shared mission-supporting IT infrastructure, and full funding would accelerate progress in this area.

The NASA CIO works with Agency leadership to develop IT modernization priorities and apply available resources. In response to the Modernizing Government Technology (MGT) Act, NASA continues to

evaluate the establishment of an IT working capital fund (WCF) authorized under 51 U.S.C. § 30102. An IT WCF could provide NASA with the flexibility and longer-term support needed in order to start to address NASA's technical deficiencies.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON SPACE AND AERONAUTICS

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

Questions for the Record to:

Mr. Seaton

Submitted by Congresswoman Wexton

1. **Is NASA providing trainings to its workforce on how to securely work remotely?**

    a. ***If So:*** **What topics are included and how often are they updated? For example, does the training including topics such as how to secure their home networks, how to safely log on to their VPN, how to manage sensitive information in a remote setting, how to ensure project continuity with children learning remotely?**

    b. **What do the trainings consist of (i.e. a live zoom call, pre-recorded trainings, supporting materials) and who is responsible for conducting them?**

    c. **Are the trainings mandatory and what percentage of the workforce have completed the training?**

    d. **Do you track the efficacy of the trainings?**

    If not: **Are there plans to establish this training for workers and what is the implementation timeline?**

NASA Response: Over the last several years, NASA has invested significantly in modernizing our network, collaboration tools, and cybersecurity capabilities that are critical to enabling NASA team members to effectively work both on site and remotely. Many employees travel occasionally and/or bring their laptops home with them often – even daily – in case of weather events or other emergencies, or simply to do work in the evening. Prior to the pandemic, NASA supported routine telework with supervisor approval. Additionally, NASA has scheduled multiple telework exercises over the last few years to test our systems and ensure that all NASA employees know how to safely connect to the NASA network when working remotely. In doing so, employees must become familiar with and utilize telework resources such as the Agency's Virtual Private Network (VPN) when connecting to internal NASA systems remotely – additional training is made available to employees before and after these telework exercises.

Annually, the NASA Office of the Chief Information Officer (OCIO) requires all civil servant and contractor employees complete annual information technology (IT) security training in order to maintain access to NASA IT resources and the corporate NASA network. This training is done via our System for Administration, Training, and Educational Resources for NASA (SATERN) online learning system and successful completion is tracked. The annual training class is not passive – users are required to watch

videos, read materials and take a test to ensure their understanding of core material. Compliance with the training requirement is mandatory and users who do not complete their training in a timely manner can have their IT access rescinded. The NASA OCIO also regularly provides communications and live training opportunities to the workforce with additional information for properly using Agency-provided collaboration tools and securing NASA data, as well as best cyber practices in general, whether at work or at home for personal use.

During the pandemic, NASA OCIO has increased training resources to employees, especially for new capabilities that were deployed during the pandemic, to include training about new collaborative tools such as Microsoft Teams and the new Microsoft Office 365 cloud-based suite of tools. Additionally, NASA OCIO has increased the number of "help desk" workers standing by to answer calls from employees who may be having problems with their IT hardware or software resources.

Responses by the Honorable Paul K. Martin

House Committee on Science, Space, and Technology
Subcommittee on Space and Aeronautics
Questions for the Record
Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19
Submitted by Chairwoman Horn

Response Provided by
Paul K. Martin
NASA Inspector General

1. Mr. Seaton's prepared testimony notes that NASA received the highest rating ("Managing Risk," the highest on a three-level scale) on its Fiscal Year (FY) 2019 Federal Information Security Modernization Act (FISMA) self-assessment. On a different scale, however, your office's independent FY2019 FISMA assessment rated NASA as Level 2 ("Defined Risk") of 5 for the fourth year in a row. What are the differences between these two assessments? Are both assessments using the same types of metrics and analyses? a. How should Congress consider these assessments, given what appear to be conflicting conclusions?

Both assessments are organized around the five core security functions outlined in the National Institute of Standards and Technology's (NIST) cybersecurity framework; however, NASA CIO's self-assessment was based on the CIO FISMA metric, while we based our assessment on the Inspector General (IG) FISMA metric. The CIO FISMA metric measures the number or percentage of users or systems that contain certain characteristics (e.g., the number of assets scanned for malware prior to an authorized remote access connection to the unclassified network). The IG FISMA metric evaluates the extent an agency has developed, implemented, and measured the effectiveness of cybersecurity policies, procedures, and controls.

NASA's self-assessed rating of "Managing Risk" is defined as the Agency instituting required cybersecurity policies, procedures, and tools and actively managing its cybersecurity risks. Our rating of "Defined (Level 2)" means the Agency's policies, procedures, and strategies are formalized and documented but not consistently implemented. Based on our assessment, NASA has generally developed required policies and procedures but has not implemented them consistently across the Agency.

2. In response to my question during the hearing, you stated that the Office of the Chief Information Officer (OCIO) does not have full insight into mission information technology (IT) infrastructure and that "the lack of insight and oversight—wielding the stick that controls the money on the end of it—is a real governance issue." Following your statement, Mr. Seaton stated that he sees "significant progress" in improving the issue. Do you agree that the changes he noted—which include placement of the CIO on various councils and collaboration with missions—have brought about "significant progress" in the areas of concern? What are the priority actions that NASA needs to take to address the governance issue?

The OIG remains both cautious and optimistic about NASA's progress related to IT governance. We see the participation of the CIO on various management councils, as well as collaboration with the Mission Directorates, as positive steps to providing the OCIO insight into Agency IT activities and spending. The OCIO has successfully addressed recommendations from our previous IT governance reports, resulting in closure of all outstanding recommendations. However, while these changes improve visibility and insight by the CIO, the decentralized nature of NASA's operations coupled with its long-standing culture of Center autonomy continue to pose challenges to the OCIO's ability to implement effective enterprise-wide IT governance. Moreover, while the improvements discussed are positive steps, it will take years for the planned and proposed solutions to achieve an appropriate level of maturity. That said, sustained senior leadership attention is key to ensuring that NASA continues to make progress in addressing its longstanding IT governance issues.

3. Your office's March 2020 report, "NASA's Management of Distributed Active Archive Centers," found shortcomings in the cybersecurity plans for the Earth Science Division's Distributed Architecture Archive Centers (DAACs) that, according to the report, could be traced, at least in part, to inadequate involvement and coordination between the program and the OCIO. What is the importance of early coordination and involvement of the agency CIO in mission and program development, and do you see evidence that NASA has improved in this area?

Early coordination and involvement between individual missions and OCIO ensures all parties are informed and have sufficient input into data management plans, which detail the types and amount of data to be collected, processed, and stored. Without this consultation, as found during our audit, missions increase the risk of schedule delays, poor data quality, or expensive redesign by the missions or the DAACs. Furthermore, involving OCIO personnel during security assessments helps ensure the systems are appropriately categorized, protecting the confidentiality, integrity, and availability of the system and its data. In June 2020, NASA took corrective action related to one of our recommendations to ensure coordination between Earth Science Data Information System personnel and the OCIO early in a mission's life cycle (during data management plan development); we view this as a positive step. However, additional work still needs to be done such as coordinating with the OCIO during the security plan review process to ensure all applicable information types are considered during system categorization, ensuring appropriate premises are used when determining impact levels, and standardizing proper categorization procedures across systems.

4. During the hearing, in responding to a question from Mr. Beyer about personal device access to NASA networks, Mr. Seaton stated that the pandemic has impacted NASA's implementation of improved procedures around network access control for personal mobile devices, including delaying the schedule to next year. What are the potential risks to its networks if NASA fails to implement these changes, or delays implementation until at least next year?

If NASA fails to fully implement improved procedures around network access control for personal mobile devices, the Agency will continue to remain at risk since it cannot ensure that only authorized IT devices are accessing its enterprise and mission networks and systems. In addition, NASA's ability to effectively monitor, detect, report, and respond to security incidents is hindered by not by having a fully-implemented network access enforcement solution. Unauthorized IT devices connecting to NASA's networks and systems can expose sensitive data and critical NASA assets to compromise or loss.

Responses by Dr. Diana L. Burley, Ph.D.

Office of Research
AMERICAN UNIVERSITY

October 27, 2020

To: Chairwoman Kendra Horn
House Committee on Science, Space, and Technology
Subcommittee on Space and Aeronautics

From: Diana L. Burley, Ph.D.
Vice Provost for Research
American University

Re: Response to Questions for the Record
September 18, 2020 Hearing Cybersecurity at NASA:
Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19

Chairwoman Horn,

I am pleased to submit the responses below to your questions for the record.

1. What is your advice to large organizations such as NASA on how to structure cybersecurity management, when weighing centralized, organization-wide approaches versus decentralized approaches with units tailoring their cybersecurity strategy to their needs?

Response: Large organizations such as NASA are well served with a hybrid approach to cybersecurity management. Top level control is essential to ensuring standard protocols and procedures. However, given the variety of functions, locations, and sub-ordinate missions, the agency needs to maintain a level of flexibility for adjustments based on the operational realities experienced within individual units.

2. Federal Information Security Modernization Act (FISMA) assessments of progress in information technology (IT) infrastructure modernization and addressing cybersecurity vulnerabilities have shown that most federal agencies are actually trending in a positive direction, but NASA is consistently faring relatively poorly in these assessments, even when compared to other R&D or high-profile agencies. What do you see is going well in federal government cybersecurity management? Are there particular approaches, technologies, strategies, or attitudes that you see contributing to the relative success or progress of most other federal agencies?

4400 Massachusetts Avenue, NW • Washington, DC 20016 • www.american.edu/research • 202-885-2935 • vpr@american.edu

Response: Any agency with the size and complexity of NASA will find it difficult to make consistent and sustained progress across all components in a given reporting period. Without direct knowledge of the practices within the agency, I am unable to comment specifically on their assessment.

3. In response to a question from Mr. Perlmutter during the hearing, you stated that ensuring adequate cybersecurity of the workforce needs to be a collaboration between an organization's information technology (IT) and human resources departments. One way you mentioned was by helping tailor cybersecurity awareness programs to the work from the home environment. What are other actions that a Human Resources department could take to help address the human factors aspect of cyber security?

Response: Human Resources (HR) departments play a critical role in identifying and addressing employee needs. Before the mass migration to remote work, it was easier to distinguish between the "work" environment and the "non-work" environment where healthcare, child and family welfare, housing stability, and other such needs take a more prominent place in the minds of employees. Given the blurring of the boundaries between these environments, cybersecurity awareness programs need to be re-envisioned and designed to address the stressors employees are facing in these blended working environments. Practicing good cyber hygiene is important, but the drivers of behaviors counter to these practices are not easily compartmentalized. Rather, they are inextricably linked to environmental realities faced by employees. HR professionals are uniquely positioned to provide insights on these environmental realities and, in turn, facilitate the design of more robust awareness programs. In addition, HR professionals can work to address and reduce the stressors that may directly impact the agency cybersecurity posture.

4. NASA has indicated in the past that some of its existing IT infrastructure is aging and may present cybersecurity risks. Do you have perspectives on the significance of aging IT infrastructure on overall cybersecurity risks?

Response: An aging IT infrastructure can present significant challenges to securing the enterprise. Older devices may not support newer encryption standards and may contain known vulnerabilities. The aging infrastructure may increase system downtime and may not be able to support increasing networking and bandwidth requirements; causing employees to seek work arounds outside of the system.

5. During the hearing, Mr. Seaton stated that while NASA has changed their "bring-your-own- device" policy in recent years, they still permit non-agency mobile devices to gain access to the network if users have download a mobile device management software. Do you have perspectives on the use of non-agency or personal devices on an agency or organization's network and the use of mobile device management software to control any associated risks?

Response: Agency policy on personal devices must consider both the ability of the system (technical infrastructure, policies and procedures) to be secured and the needs of the employees. NASA, as with every other enterprise, must balance these (often) competing demands based on their best judgement and the risk appetite of the senior leaders. No one size fits all solution exists.

Thank you for the opportunity to appear before the Committee and to respond to the questions above for the record. I appreciate the Committee's commitment to addressing the cybersecurity challenges and emerging issues for increased telework during COVID-19. I trust that my remarks at the hearing and in this document will enhance our ability to safeguard the American people.

4400 Massachusetts Avenue, NW • Washington, DC 20016 • www.american.edu/research • 202-885-2935 • vpr@american.edu