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.