NASA OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS
SUITE 8U71, 300 E ST SW
WASHINGTON, DC 20546-0001

May 28, 2026

TO: Sean Gallagher
Acting Chief Information Officer

SUBJECT: Final Memorandum, *NASA's Management of Elevated Privileges for Information Systems* (Report No. IG-26-008; Assignment No. A-25-08-00-MSD)

The Office of Inspector General has concluded its audit of NASA's management of elevated privileges for information systems. Elevated privileges grant users broad authority to modify configurations, access sensitive data, and control critical system functions of NASA information systems. While necessary for managing and maintaining individual computers, the increased access levels introduce significant security and operational risks if not properly controlled. Our previous audit work has identified issues with the Agency's use of elevated privileges.

In this audit, we determined whether elevated privileges for employee computers were appropriately managed, authorized, provisioned, monitored, and deprovisioned in accordance with established policies, procedures, and the principle of least privilege.[1] Specifically, we focused on two elevated privileges accounts—Workstation & Collaboration Services (WCS) Elevated Privileges and Workstation Administrator—that grant users varying levels of local administrative rights to their NASA-provided computers.[2] See Enclosure I for details of the audit's scope and methodology.

[1] Least privilege is a security principle that states a system should restrict access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

[2] The Office of the Chief Information Officer's Workplace & Collaboration Services is responsible for administration of NASA's end user services to include identity, credential, and access management services. WCS Elevated Privileges and Workstation Administrator are the names of two elevated privileges accounts available to users of NASA computers.

Background

NASA grants elevated privileges to users mainly for the purpose of downloading, installing, and updating software that has not been previously approved on their computers. A WCS Elevated Privileges account grants broad local administrator rights for a user's computer. During 2022, the Agency introduced the Workstation Administrator account, providing a reduced level of access compared to WCS Elevated Privileges. This account is designed to allow users to manage the software needed to perform their duties, while limiting the cybersecurity risk inherent with broader administrative rights.

NASA policy outlines access requirements to meet federal requirements established by the Office of Management and Budget and National Institute of Standards and Technology. NASA Procedural Requirements 2841.1, *Identity, Credential, and Access Management*, sets the requirements for the proper management of identity, credential, and access services and defines the responsibility and requirements of access to the Agency's information technology assets.[3] The Access Control – Managed Elevated Privileges handbook provides guidance on the implementation of NASA's information security controls related to elevated privileges.[4]

Elevated privileges for NASA users are administered by the Agency's Office of the Chief Information Officer. The process of requesting elevated privileges starts with the individual user completing required training for the type of elevated privileges being requested using the Agency's SATERN training platform.[5] Once access is requested by the user, a NASA Access Management System workflow—which the Agency uses to manage elevated privileges—is created. Supervisor approval is required, and if received, an organization-level approver begins the provisioning process to provide access rights to the user.[6] Organization-level approvers are typically those with administrative responsibility for their organization's information technology assets. Approvers are provided specific role-based training depending on their level of responsibility, and training requires periodic revalidation using SATERN. While the processes for provisioning and deprovisioning (providing and removing access rights, respectively) utilize automation, organization-level approvers are ultimately responsible for the management of elevated privileges for their organization.[7]

Previous audits conducted by our office have identified concerns with the Agency's use of elevated privileges. For instance, in a 2022 report we found that accessing information technology systems with elevated privileges greatly increases the risks of cybersecurity incidents by introducing unintended, detrimental changes to system configurations.[8] A user accessing a computer with elevated privileges can access, alter, and delete critical data; exploit bugs; and exploit design flaws. Additionally, in a 2023 report we found that at one NASA center, all of its approximately 6,500 users had been granted elevated privileges to download and install software at will.[9] The Agency has since taken action to remediate the risk associated with this center's employees having elevated privileges and our recommendation for this issue has been closed.

---

[3] NASA Procedural Requirements 2841.1, *Identity, Credential, and Access Management (Revalidated w/change 2)* (January 6, 2011).

[4] NASA ITS-HBK-2810.15-02, *Access Control – Managed Elevated Privileges* (November 17, 2025).

[5] SATERN is NASA's Learning Management System that provides web-based access to training and career development resources.

[6] Provisioning is the process of granting, configuring, and assigning access rights.

[7] Deprovisioning is the removal of access upon termination of, or change to, a user's employment, contract, or agreement.

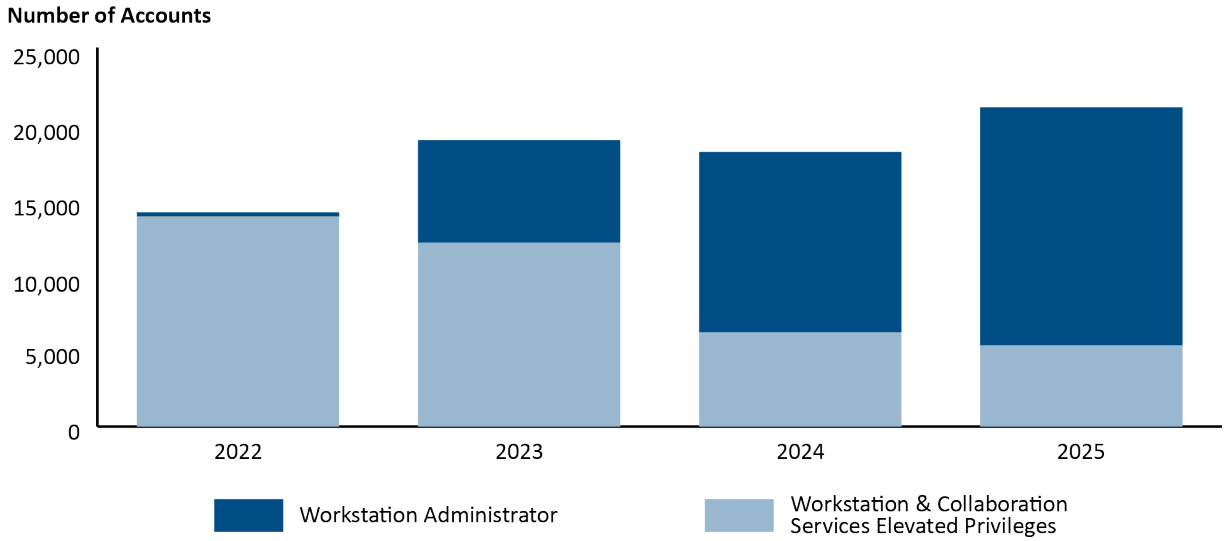
[8] NASA Office of Inspector General, *NASA's Insider Threat Program* (IG-22-009, March 14, 2022).

[9] NASA Office of Inspector General, *NASA's Software Asset Management* (IG-23-008, January 12, 2023).

NASA IS EFFECTIVELY MANAGING WCS ELEVATED PRIVILEGES AND WORKSTATION ADMINISTRATOR ACCOUNTS

Overall, we found that the Agency's process for granting WCS Elevated Privileges accounts and Workstation Administrator accounts is effective. NASA maintains an inventory of users granted elevated privileges—from 2022 to 2025, there were a total of 71,948 WCS Elevated Privileges and Workstation Administrator accounts provisioned.[10] During this time, NASA transitioned from primarily granting NASA users WCS Elevated Privileges accounts to predominantly assigning Workstation Administrator accounts (see Figure 1). These actions align with the principle of least privilege by providing elevated privileges only when necessary and for the minimum time needed.

Figure 1: WCS Elevated Privileges and Workstation Administrator Accounts 2022 to 2025



Source: NASA Office of Inspector General summary of Agency data.

The number of WCS Elevated Privileges accounts provisioned fell from 13,875 accounts in 2022 to 5,385 in 2025. Conversely, the number of Workstation Administrator accounts provisioned rose from 5 in 2022 to 15,698 in 2025. Data regarding deprovisioning of the two accounts aligns with the provisioning—in that as time goes on, more of the deprovisioning is completed for Workstation Administrator than WCS Elevated Privileges—suggesting shortened time frames for local administrative access to a user's computer.

We determined that NASA has established policies and procedures governing elevated privileges for WCS Elevated Privileges accounts and Workstation Administrator accounts. Provisioning of both accounts was performed in accordance with processes established in the Managed Elevated Privileges handbook and NASA Procedural Requirements 2841.1. We also found that elevated privileges generally align with a user's job responsibilities and are restricted to users with a documented business need. WCS Elevated Privileges and Workstation Administrator accounts are also limited to the time needed to perform the required elevated privileges actions.

[10] The total includes accounts previously provisioned that were renewed between 2022 to 2025.

We have communicated our conclusions to the appropriate Office of the Chief Information Officer officials. We will continue to review the Agency's management of elevated privileges through annual Federal Information Security Modernization Act evaluations and broader reviews of privileged access management.

If you have questions or wish to comment on the quality or usefulness of this memorandum, contact Laurence Hawkins, Financial Oversight and Audit Quality Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Brian Mullins
Deputy Assistant Inspector General for Audits

Enclosure—1

Enclosure I: Scope and Methodology

While we performed this audit from September 2025 through March 2026, it was temporarily suspended during the government shutdown that occurred from October 1 to November 12, 2025. The audit was performed in accordance with generally accepted government auditing standards, which require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

Our audit scope encompassed a review of Agency processes for managing elevated privileges in the NASA Access Management System for the period of January 2022 to December 2025. Specifically, we focused on two elevated privileges accounts, WCS Elevated Privileges and Workstation Administrator. The audit covered users of NASA-provided computers and did not include hardware and software provided solely for mission use. We assessed controls against federal criteria and NASA policy, including the following:

- National Institute of Standards and Technology Special Publication 800.53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
- National Institute of Standards and Technology Federal Information Processing Standards Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (January 2022)
- NASA Procedural Requirements 1600.3B, *Personnel Security* (June 6, 2025)
- NASA Procedural Requirements 2841.1, *Identity, Credential, and Access Management* (Revalidated w/change 2) (January 6, 2011)
- NASA ITS-HBK-2810.15-02, *Access Control – Managed Elevated Privileges* (November 17, 2025)

To gain an understanding of NASA's current process for managing elevated privileges to the WCS Elevated Privileges and Workstation Administrator accounts, we conducted interviews with Agency and contractor representatives responsible for granting, removing, and administering access to these accounts. We also reviewed relevant NASA policies and procedures governing privileged account management. Additionally, we tested a sample of privileged accounts across a range of Agency organizations to determine whether controls over elevated privileges were operating as intended and analyzed historical account provisioning and deprovisioning data to provide insights and trends into WCS Elevated Privileges and Workstation Administrator accounts. As a result of these procedures, we obtained sufficient, appropriate evidence to provide a reasonable basis for our conclusions related to our evaluation objectives.

Assessment of Data Reliability

We used limited computer-processed data extracted from NASA's information technology systems during this audit. Although we did not independently verify the reliability for all the information provided, we compared it with other available supporting documents to determine data consistency and reasonableness. From these efforts, we believe the information we obtained is sufficiently reliable for this audit.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. Specifically, we assessed the control activities component relating to the design of control activities to mitigate risks and achieve objectives and respond to risks and implement control activities through policies.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General issued four reports of significant relevance to the subject of this memorandum. Reports and memorandums can be accessed at https://oig.nasa.gov/audits/.

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2025 (IG-25-007, July 29, 2025)

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2024 (IG-24-019, September 12, 2024)

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

NASA's Insider Threat Program (IG-22-009, March 14, 2022)