
DOE SBIR/STTR CYBERSECURITY SERIES
FY 2025 Phase II Release 2 Applied Offices
VIDEO 5 OF 8

Access Controls: Admin Accounts and Least Privilege

TOPIC

Separating everyday and administrator accounts, and giving people only the access they need

Practices 2.1 and 2.2 · Tier 2

Please send your Questions/Feedback to csduediligence@doe.gov



Every Extra Permission Is Something an Attacker Can Use

WHY IT MATTERS

01

Admin rights

If an admin account is taken over, the attacker gets admin powers too.

02

Leftover access

Former employees and vendors who can still log in are an open door.

03

Too much access

When everyone can see everything, more people can leak or lose your IP.



Separate User and Privileged Administrator Accounts

TIER 2 • PRACTICE 2.1

WHAT IT MEANS

Give administrators a normal account for everyday work and a separate privileged account used only for admin tasks.

HOW TO DO IT

- 1 Use standard accounts for email, web browsing, Microsoft Office/Teams, research, and normal business
- 2 Use privileged accounts only for account admin, installs and updates, firewall and security settings, patching, cloud admin, and lab system admin
- 3 Protect privileged accounts with MFA and strong, unique credentials; never share them
- 4 Log privileged actions where supported, and review admin accounts and permissions regularly
- 5 Remove privileged access immediately when duties change or people leave

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 1.0 Access Controls



The Same Phishing Click, Two Different Outcomes

PRACTICE 2.1 • WHY TWO ACCOUNTS?

ONE ACCOUNT FOR EVERYTHING

Full admin powers exposed

An admin opens a phishing email while signed in with full admin rights. The attacker now has admin powers across your systems.

SEPARATE ACCOUNTS

The damage is contained

The same click happens in an everyday account. The attacker gets limited access, and admin systems stay out of reach.



Implementation Steps

PRACTICE 2.1 • STEP BY STEP

01

Find high-value systems

Email, cloud storage, code platforms, research and lab systems, finance/HR, cloud admin portals.

02

List current admins

Everyone with administrator, owner, root, super-admin, or global-admin rights.

03

Create separate accounts

A standard account for daily work; a privileged one only for admin tasks.

04

Lock down admin accounts

MFA on every privileged account, and no shared admin credentials.



Implement the Principles of Least Privilege

TIER 2 • PRACTICE 2.2

WHAT IT MEANS

Give users, administrators, applications, service accounts, and system processes only the access they need to do their job.

HOW TO DO IT

- 1 Grant access based on job need, using roles or groups where practical
- 2 Don't give admin rights unless required; stop standard users from privileged actions unless approved
- 3 Limit service accounts to the permissions they need, and protect their credentials
- 4 Review access and role assignments quarterly (CISA CPG 2.0) and remove what isn't needed
- 5 Change or remove access immediately when people leave or change roles; log and review privileged activity
- 6 Record who approved privileged access, what it covers, and when it was last reviewed

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 2.2



Can a Third-Party Service Provider Help?

PRACTICES 2.1 & 2.2 • GETTING HELP

SERVICE	WHAT TO DO IN THE SERVICE
Microsoft 365 / Entra	Assign only the Entra roles people need, use separate administrator accounts, require MFA for admins, and review role assignments.
Google Workspace	Use admin roles with only the privileges needed, avoid using a super-admin account for daily work, and enforce 2-Step Verification for admins.
AWS	Use IAM roles and policies that grant least privilege, protect privileged identities with MFA, and avoid routine use of the root user.

The service provides the features; your company still selects the settings, assigns responsible people, reviews reports, and documents that it works.



What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Former employees or vendors can still reach your systems and data.
- A single phished admin account can compromise everything.
- People can see, copy, or leak IP they never needed.

To your DOE SBIR/STTR award

- Gaps can come to light during a DOE on-site review or audit.
- You won't have the evidence the form says you can produce.
- Your signed Management Review would describe practices that aren't really in place.



What to Show DOE for Each Practice

EVIDENCE TO KEEP READY

PRACTICE	EVIDENCE (FROM THE EVIDENCE FORM)
2.1 Separate admin accounts	Access control policy and/or policy that describes separating user and privileged administrator accounts
2.2 Least privilege	Access-control policy and/or process that describes how principles of least privilege are implemented

Guide estimate: 8–24 hours of hands-on effort over 1–3 business days for access controls.



Remember These

KEY TAKEAWAYS

- 1 Admins get two accounts, and admin work happens only in one
- 2 Give only the access each job needs
- 3 Review access every quarter, and the same day someone leaves
- 4 Protect every privileged account with MFA

Up next • Video 6: Secure Data: Email Security and Encryption

Please send your Questions/Feedback to csduediligence@doe.gov

