
DOE SBIR/STTR CYBERSECURITY SERIES
FY 2025 Phase II Release 2 Applied Offices
VIDEO 7 OF 8

Unsuccessful-Login Monitoring: Stop Password Guessing

TOPIC

Detecting repeated failed sign-ins and stopping password-guessing attacks before they succeed

Practice 2.5 · Tier 2

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



Failed Logins Are an Early Warning

WHY IT MATTERS

01

Brute force

Many password guesses against one account.

02

Password spraying

A few common passwords tried against many accounts.

03

Credential attacks

Passwords stolen from other breaches tried on your systems.



Monitor Unsuccessful Login Attempts

TIER 2 • PRACTICE 2.5

WHAT IT MEANS

Detect repeated failed sign-ins and automatically slow, block, lock, or alert on suspicious attempts before an attacker gains access.

HOW TO DO IT

- 1 Write down how failed login attempts are monitored and handled
- 2 Capture failed logins for important systems: user and admin accounts, VPN, cloud services, and email
- 3 Set a number of failed tries in a time period that triggers a lockout, delay, alert, or other documented response
- 4 Alert IT or security on suspicious patterns, and keep the alert in a security or ticketing system
- 5 Review failed-login activity regularly, investigate anything odd, and record what you fixed

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 3.0 Unsuccessful-Login Monitoring



Implementation Steps

PRACTICE 2.5 • STEP BY STEP

01

Find the systems that matter

Email, cloud identity, VPN, remote access, research servers, and admin portals.

02

Set limits

Limit repeated failures in a set period, with an automatic lockout, delay, or other response.

03

Turn on logging

Record user and administrator sign-ins.

04

Alert on patterns

Repeated failures, unusual sign-ins, password spraying, attacks on admin accounts.

05

Assign a reviewer

Name the person or provider who reviews alerts, and what needs investigating.

06

Respond

Preserve logs, reset or disable credentials, revoke sessions, and document it.

07

Test it

Periodically confirm the protections and logging still work.



Choosing Your Lockout Settings

PRACTICE 2.5 • SETTINGS

01

You set the number

NIST SP 800-171 Rev. 3 requires you to define the number of failed attempts and the response. There's no single number for everyone.

02

Pick the response

Temporary lockout, delay or throttling, an administrator alert, or another documented measure.

03

Keep the record

Retain alerts and logs in a security or ticketing system so you can show what happened.



Can a Third-Party Service Provider Help?

PRACTICE 2.5 • GETTING HELP

SERVICE	WHAT TO DO IN THE SERVICE
Microsoft Entra ID / Microsoft 365	Use smart lockout and the identity protection and sign-in logs available to your tenant; set alerts and review risky or repeated sign-ins.
Google Workspace	Use the login audit and security investigation tools for your edition; review failed or suspicious logins and set alert rules where supported.
AWS	Use CloudTrail and IAM security services to record and investigate sign-in and API activity; set alarms that fit your environment.



What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Password-guessing attacks go unnoticed until the damage is done.
- A taken-over account can expose research, IP, and CUI.
- Without logs, you can't tell what happened or prove it.

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)
2.5 Failed login monitoring	Login/lockout policy

Guide estimate: 1–3 hours for one cloud identity platform; 4–8 hours when several systems, VPNs, servers, or research apps must be configured.



Remember These

KEY TAKEAWAYS

- 1 Log failed sign-ins on every important system
- 2 Set a limit with an automatic lockout, delay, or alert
- 3 Name who reviews the alerts, and act on them
- 4 Write it down in a login/lockout policy

Up next • Video 8: Incident Response: Your Plan and Procedures

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

