DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

VIDEO 3 OF 8

Secure Devices and Accounts: Passwords and MFA

TOPIC

Closing the most common doors attackers use: factory passwords, weak passwords, and single-factor logins

Practices 1.4, 1.5, and 1.6 · Tier 1

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

Attackers Would Rather Log In Than Break In

WHY IT MATTERS

01

Default passwords

Factory passwords and accounts are printed in manuals and easy to find online.

02

Weak or reused passwords

Short passwords get guessed; reused ones leak from other sites' breaches.

03

No second factor

Without MFA, a stolen password is all an attacker needs.

Change or Disable Default Passwords and Accounts

TIER 1 · PRACTICE 1.4

WHAT IT MEANS

Change or disable factory default passwords, accounts, and logins before a system goes into use or connects to your network.

HOW TO DO IT

1. Install current security updates before the device goes live
2. Run a vulnerability scan and patch the weaknesses it finds
3. Change defaults on routers, firewalls, Wi-Fi, NAS, printers, VoIP phones, lab equipment, IoT, apps, databases, VMs, and cloud services
4. Disable unneeded default, guest, and test accounts; secure any that can't be removed and add MFA
5. Check the change worked before use, and record it in your setup process
6. Can't change it? Document why, add other protections and monitoring, and plan a replacement

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 3.0 Secure Devices and Accounts

Implementation Steps

PRACTICE 1.4 · STEP BY STEP

01
Update first
Apply the vendor's recommended updates.

02
Scan for weaknesses
Run a vulnerability scan, patch, and repeat periodically.

03
Sign in with the default
Use the initial administrator login one last time.

04
Create a named admin
Set up a named company admin account where supported.

05
Set a strong password
Unique passphrase, saved in the business password manager.

06
Remove extras
Disable default, guest, and test accounts you don't need.

07
Turn on admin MFA
Wherever the product supports it.

08
Verify and record
Confirm it, and note the date in your inventory.

09
Legacy device?
Isolate, monitor, document, and plan to replace it.

Establish and Enforce Minimum Password Strength

TIER 1 · PRACTICE 1.5

WHAT IT MEANS

Set and enforce a password policy that makes passwords hard to guess or crack.

HOW TO DO IT

1. Require 16 or more characters wherever the system allows (CISA CPG 2.0)
2. Encourage long passphrases and provide an approved password manager
3. Use a unique password for every business account; never reuse it on personal accounts
4. Block common, expected, or compromised passwords where the platform supports it
5. Don't force changes just because time passed; change after compromise, exposure, or recovery
6. Can't reach 16 characters? Document it, add MFA, log login attempts, and plan an upgrade

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 1.5

Where Strong Passwords Get Set Up

PRACTICE 1.5 · GETTING HELP

01

Microsoft 365 / Entra

Use Entra password protection where available, keep password expiration off unless required, and pair passwords with MFA.

02

Google Workspace

Use Admin console password settings, enforce 2-Step Verification, and reset passwords if compromise is suspected.

03

Password manager

Approved company vault with unique generated passwords, protected by MFA. It supports MFA; it doesn't replace it.

04

Your MSP

Can configure the settings and give you a screenshot or export. You approve the policy and keep the evidence.

Implement Multi-Factor Authentication (MFA)

TIER 1 · PRACTICE 1.6

WHAT IT MEANS

Require MFA to access your business and work systems, using the strongest method available. A password alone should not be enough.

HOW TO DO IT

1. Require MFA for every employee account on systems with federal contract or sensitive information or CUI, and for every admin account
2. Turn it on for email, cloud platforms, VPN/remote access, file sharing, and systems with federally funded R&D, IP, or CUI
3. Prefer phishing-resistant passkeys, security keys (FIDO), or PKI; otherwise use app prompts with number matching, not text or voice
4. Document how authenticators are issued, replaced, recovered, and excepted
5. Review accounts regularly to confirm MFA stays on and remove unapproved exceptions

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 1.6

Turning On MFA in Common Services

PRACTICE 1.6 · GETTING HELP

01

Microsoft 365 / Entra

Security Defaults (free baseline) or Conditional Access (Entra ID P1/P2). Legacy per-user MFA isn't recommended. Microsoft MFA setup

02

Google Workspace

Enforce 2-Step Verification. Security keys are strongest; passkeys are available; avoid text messages. Google 2-Step Verification

03

AWS

Require MFA through IAM or IAM Identity Center. Protect the root user with strong MFA and avoid using it day to day.

04

VPN, remote access, MSP portals

Turn on MFA or single sign-on, ideally through your Microsoft or Google identity. Cover every remote and admin path, including vendor accounts.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Attackers log in with factory, guessed, or stolen passwords.
- A compromised email account can be used to trick customers and partners.
- One stolen password can expose research, IP, and CUI.
- Loss of intellectual property can harm your business.

To your DOE SBIR/STTR award

- Your Tier 1 submission may not be approved, and Tier 2 can't start until it is.
- Missing evidence can come to light during a DOE on-site review.
- 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)
1.4 Default passwords	Password policy and/or process that addresses changing default passwords
1.5 Password strength	Password management policy that addresses establishing minimum password strength
1.6 MFA	MFA process and/or policy (the guide suggests including documented exceptions and a recovery procedure)

Guide estimates: defaults 2–8 hours total; password policy 1–3 hours (1–5 days if many apps); MFA 2–4 hours plus user enrollment (1–7 business days).

Remember These

KEY TAKEAWAYS

1. Change or disable every default password and account before use
2. Require long, unique passwords, plus a password manager
3. Put MFA on every account, phishing-resistant where possible
4. Document exceptions, and review them regularly

Up next · Video 4: Backups and Restoration: Be Ready to Recover

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