DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

VIDEO 4 OF 8

Backups and Restoration: Be Ready to Recover

TOPIC

Making reliable, protected copies of what you need, and proving you can restore them

Practice 1.7 · Tier 1

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

Plan for a Bad Day Before It Happens

WHY IT MATTERS

01

Ransomware

Files are locked, and research stops until they're restored.

02

Hardware failure

A server, laptop, or instrument dies and takes its data with it.

03

Accidental loss

Someone deletes or overwrites data that's hard to recreate.

Maintain System Backups & Restoration Ability

TIER 1 · PRACTICE 1.7

WHAT IT MEANS

Back up the information and settings you need to restore R&D operations after a cyberattack such as ransomware, a hardware failure, or accidental loss.

HOW TO DO IT

1. Identify what needs backup: systems, apps, research data, IP, CUI, settings, install media, and recovery information
2. Back up on a schedule based on importance; critical systems may need more frequent backups
3. Keep at least one protected copy separate from everyday systems, offsite or offline (CISA CPG 2.0)
4. Protect sensitive backups, including with encryption where applicable
5. Test restoring at least once a year; check the data is complete and not corrupted before use
6. Record test results, fix problems, and review the process yearly and after big changes

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 4.0 Maintain Backups and Restoration Ability

Implementation Steps

PRACTICE 1.7 · STEP BY STEP

01

Use your inventory

Pick what to back up: research data, IP, code, settings, servers, CUI.

02

Set a schedule

Base it on how much data you can afford to lose. Critical data may need daily backups.

03

Keep a separate copy

Logically or physically separate, and deletion-protected where available.

04

Limit backup admins

Only authorized people, and require MFA for them.

05

Encrypt and protect keys

Encrypt backups when appropriate; guard recovery credentials.

06

Test a restore

Restore a sample file or system. Is it complete, readable, accurate, usable?

07

Record the test

Date, who did it, what was restored, result, problems, and fixes.

08

Review yearly

And after significant changes.

Built-In Retention Isn't Always a Backup

PRACTICE 1.7 · CLOUD APPS

BUILT-IN FEATURES

Recycle bins and retention

Microsoft 365 and Google Workspace have recovery and retention features, but these aren't always a complete backup that meets your recovery needs.

A REAL BACKUP PLAN

Dedicated backup, tested

A backup with a defined scope, schedule, retention, protected copies, and restore tests you have actually done.

Common Cloud Options

PRACTICE 1.7 · GETTING HELP

SERVICE	HOW IT CAN HELP	KEEP IN MIND
Microsoft 365	Retention and recovery features, plus Microsoft 365 Backup or an approved third-party backup.	Retention isn't the same as a backup strategy; test restores.
Google Workspace	Native recovery features for your edition, plus a dedicated Workspace backup when needed.	Service availability isn't a complete backup.
AWS	AWS Backup plans, schedules, retention, vault controls, and protected copies.	You choose resources, schedules, permissions, and tests.
Azure	Azure Backup / Recovery Services policies, protected items, and retention.	Confirm it covers each workload and data type.
MSP / backup vendor	Documents scope, frequency, retention, separation, monitoring, failed jobs, and restore tests.	Get the evidence and take part in restore tests.

What Counts as Good Evidence?

TIER 1 GUIDE · EVIDENCE TIPS

01

Policy and proof

Good evidence shows the written expectation and the actual setting. A policy by itself is acceptable to the SBIR/STTR Office.

02

Restore test records

Keep the date, who tested, what was restored, the result, and any fixes.

03

Redact secrets

Remove passwords, private keys, recovery codes, tokens, and unneeded personal information before you submit.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Ransomware without a working backup can mean lost research.
- Backups stored with everyday systems can be encrypted or deleted too.
- Untested backups may fail when you need them most.

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)
1.7 Backups and restoration	Backup/restore process and/or policy

Guide estimate: 3–10 hours for setup and a sample restore test; 1–10 business days depending on data volume and test scheduling.

Remember These

KEY TAKEAWAYS

1. Back up what you need to restore R&D operations
2. Keep one protected copy separate, offsite or offline
3. Test a restore at least once a year, and record it
4. Tier 1 is complete: submit it for SBIR/STTR Office approval before Tier 2

Up next · Video 5: Access Controls: Admin Accounts and Least Privilege

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