DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

VIDEO 1 OF 8

Cybersecurity Leadership: Your Lead and Program

TOPIC

Naming a Cybersecurity Lead and running a simple, documented cybersecurity program

Practice 1.1 · Tier 1

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

One Person Must Be Accountable

WHY IT MATTERS

01

Someone owns it

Name one person who is accountable for cybersecurity, so tasks don't fall through the cracks.

02

Small company options

Often the owner, Principal Investigator (PI), operations lead, or an IT or security employee.

03

Providers can help

An MSP or consultant may do technical work, but your own leader stays accountable.

04

What stays with you

Oversight, decisions, accepting risk, resources, and evidence.

Establish Cybersecurity Responsibilities

TIER 1 · PRACTICE 1.1

WHAT IT MEANS

Appoint a Cybersecurity Lead with the responsibility and authority to manage your company's cybersecurity program.

HOW TO DO IT

1. Record the lead's name, role, and backup contact information
2. Develop and enforce cybersecurity awareness training
3. Keep a cybersecurity plan showing how you'll meet the Tier 1 and Tier 2 practices to protect systems, research data, IP, and CUI
4. Write, approve, share, and regularly review your cybersecurity policies
5. Do and document regular risk assessments; check your safeguards are working
6. Track weaknesses and fixes to closure, and update the program after big changes

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 1.0 Cybersecurity Leadership

What the Cybersecurity Lead Is Responsible For

PRACTICE 1.1 · THE LEAD'S JOB

01

Plan and inventory

Keep the cybersecurity plan and the asset inventory up to date.

02

Accounts and access

Review who has accounts and what they can reach.

03

Risk and weaknesses

Run risk assessments and track vulnerabilities until they're fixed.

04

Backups and providers

Make sure backups work and service providers are overseen.

05

Incidents and insiders

Keep the company ready for incidents and manage insider threats.

06

Evidence

Collect and keep the proof DOE may ask to see.

What the SBC Should Do

PRACTICE 1.1 · GETTING STARTED

01
Appoint the lead in writing
Record name, role, authority, backup contact, and date assigned.

02
Define the duties
List what the lead owns: plan, inventory, reviews, risk, backups, providers, incidents, evidence.

03
Identify what you protect
Research data, IP, proposal and award information, business data, and CUI if applicable.

04
Write a simple plan
Describe your environment and how each required practice is put in place.

05
Set a review schedule
At least yearly, and after major changes, incidents, new providers, or moves.

06
Verify independently
Periodically have your controls checked through an independent assessment.

07
Track open gaps
Keep a corrective-action list with an owner and target date for each item.

Conduct Risk Assessments

PRACTICE 1.1 · CONDUCT RISK ASSESSMENTS

01

Assess regularly

Do periodic security assessments to confirm your controls are in place and working.
Guide: NIST SP 800-30 Rev. 1, Conducting Risk Assessments

02

Test where risk calls for it

Do penetration testing when your level of risk warrants it.

03

Track to closure

Log every finding in a remediation tracker, such as a plan of action and milestones (POA&M), until it's fixed.

Conduct Cybersecurity Awareness Training

PRACTICE 1.1 · AWARENESS TRAINING

01

Protect logins

Train employees to protect against credential theft.

02

Spot the threats

Teach people to recognize phishing, insider threats, and data-handling risks.

03

Test what they learned

Run periodic exercises, such as simulated phishing emails.

04

Write down the program

Document your training requirements. The form asks you to submit them as evidence.

Can a Third-Party Service Provider Help?

PRACTICE 1.1 · GETTING HELP

SERVICE	HOW IT CAN HELP	KEEP IN MIND
MSP / MSSP	Often a lot: patching, device management, accounts, log review, backups, scanning. Put duties in the contract.	Don't make the MSP the only owner of compliance or risk decisions.
Microsoft 365 / Entra	Admin roles, security reports, MFA, access controls, and audit tools support the lead's work.	Features vary by license; you assign and review roles.
Google Workspace	Admin roles, 2-Step Verification, security reporting, and organization settings.	Defaults alone may not meet the goal; you configure and enforce.
AWS / Azure / other cloud	Identity and access management, logging, configuration, and backup tools, with named owners.	The provider's security doesn't secure your accounts, data, or settings.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- No one is accountable, so security tasks quietly fall through the cracks.
- Untrained staff are more likely to fall for phishing and credential theft.
- Risks and weaknesses go unnoticed or are found and never fixed.
- 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)
1.1 Cybersecurity Lead	Cybersecurity personnel information (template provided by SBIR/STTR Office)
1.1 Corrective actions	Corrective action list (template provided by SBIR/STTR Office)
1.1 Cybersecurity plan	Cybersecurity plan (template provided by SBIR/STTR Office)
1.1 Awareness training	Cybersecurity training awareness program requirements

Guide estimate: 2–6 hours if roles and systems are known; 1–3 business days if leadership approval or an MSP review is needed.

Remember These

KEY TAKEAWAYS

1. Name one Cybersecurity Lead in writing, plus a backup
2. Keep a simple plan, written policies, and a corrective-action list
3. Train your people, and test them
4. Assess risk regularly and fix what you find

Up next · Video 2: Know What You Have: Assets, Data, and Providers

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