DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

Introduction: How the Cybersecurity Process Works

TOPIC

How the evidence form and supplemental guides work, and what DOE expects from your small business

Evidence Form · Tier 1 and Tier 2 Supplemental Guides

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

How to Use Implementation & Evidence Form

01

Fill in your company details

Complete the small business award information and the environment profile.

02

Read the guidance

For each DOE requirement, read the implementation guidance in the form.

03

Use the supplemental guide

Need more detail? See the DOE SBIR/STTR Supplemental Guide for Tier 1 (and Tier 2) practices.

04

Attach your evidence

Attach or identify proof for each practice. A written policy or proof that it's working may be enough.

05

Tier 1 comes first

The SBIR/STTR Office must approve your Tier 1 practices before you begin Tier 2.

06

Sign the Management Review

Your Cybersecurity Lead and PI or business official confirm the form is accurate, and you update it as things change.

What does Supplemental Guides cover?

Tier 1 Guide: four areas

- 1.0 Cybersecurity Leadership
- 2.0 Manage Organizational Assets, Data, and Service Providers
- 3.0 Secure Devices and Accounts
- 4.0 Maintain Backups & Restoration Ability

Tier 2 Guide: four areas

- 1.0 Access Controls
- 2.0 Secure Data (email security and encryption)
- 3.0 Unsuccessful-Login Monitoring
- 4.0 Incident Response

Please note: A service provider can supply a security feature, but your company must make sure it's turned on, set up correctly, applied to the right people and systems, reviewed, and documented. Outsourcing IT does not outsource accountability.

What "Fully Implemented" Should Mean for an SBC

EVIDENCE FORM · TIER 1 & 2 GUIDES

01

It's turned on

The setting or process is enabled and working on the systems in scope.

02

Someone owns it

An employee, owner, IT administrator, MSP, or MSSP is responsible for it.

03

It's written down

A short policy, procedure, or configuration record describes it.

04

People know it

Everyone who must follow the practice knows what's expected.

05

You can prove it

Screenshots, exported settings, logs, reports, tickets, policies, or test results.

06

It's kept current

Reviewed regularly, and after big system, staff, or service changes.

07

It protects the data

Strong enough to keep CUI, FCI, and sensitive information from unauthorized disclosure.

08

Remember

A practice counts only when all of these are true, not just when a feature exists.

Framework Alignment Note

EVIDENCE FORM

DOE's tier requirements are the rules that count. The form also points to CISA's Cybersecurity Performance Goals (CPG 2.0) and NIST SP 800-171 Rev. 3 to explain the expected outcome and evidence.

NIST SP 800-171 Rev. 3 applies to systems that process, store, send, or protect CUI. The NIST references in this form are alignment aids and should not be read as automatically imposing every NIST requirement on an awardee that does not handle CUI.

REFERENCES

CISA Cybersecurity Performance Goals (CPG 2.0)
Measurable, foundational security goals
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

NIST SP 800-171 Rev. 3
Protecting CUI in nonfederal systems
https://csrc.nist.gov/pubs/sp/800/171/r3/final

NIST SP 1318
NIST SP 800-171 Rev. 3 Small Business Primer
https://csrc.nist.gov/pubs/sp/1318/final

NIST SP 800-171A Rev. 3
How CUI requirements are assessed
https://csrc.nist.gov/pubs/sp/800/171/a/r3/final

Important Scope Note

TIER 1 & 2 GUIDES

IF YOU HANDLE CUI

NIST SP 800-171 Rev. 3 applies

It applies to the systems that process, store, send, or protect CUI. Also confirm your contract requirements, system boundary, cloud and provider use, and any required federal authorizations.

IF YOU DON'T HANDLE CUI

These practices still matter

They're a strong baseline for protecting federally funded research, intellectual property, proposal information, business information, and other sensitive data.

Small Business Environment and Scope

EVIDENCE FORM · SECTION 2

SECTION	WHAT TO DESCRIBE
Small Business Environment	Where and how the work is done. List the computers, servers, cloud services, networks, and other technology that handle business information, intellectual property, and CUI. This isn't limited to computers or a physical office.
Protected Information	The types of data you use: federally funded research, intellectual property and source code, engineering and scientific data, business and sensitive information, FCI, and CUI if applicable. Unsure? See the Tier 1 Supplemental Guide.
Managed / Cloud Services	Every provider that runs, hosts, stores, processes, monitors, or remotely accesses your systems or data: MSP/MSSP, email, collaboration, cloud storage, source code, backups, business apps, communication, AI services, and research platforms.

Small Business Environment and Scope: Example

EVIDENCE FORM · SECTION 2

SECTION	EXAMPLE ANSWER
Small Business Environment	We are a five-person company that uses home office networks to operate the business. We use company laptops, cloud storage, research systems, source-code repositories, network infrastructure, remote access, backups, relevant laboratory systems, and third-party services with access.
Protected Information	Our systems process research and development data, intellectual property, source code, business-sensitive information (pricing, financial information, business strategies), prototype/test information, and personnel information.
Managed / Cloud Services	Our cloud infrastructure is AWS, Google Cloud, and Microsoft Azure. We use Microsoft 365 and Google Workspace for email and collaboration, Google Drive and OneDrive for files, GitHub for source code, Microsoft 365 and AWS for backups, QuickBooks Online, and Microsoft Teams.

Tier 1 Quick Planning Estimate

TIER 1 SUPPLEMENTAL GUIDE

PRACTICE	TYPICAL HANDS-ON EFFORT	TYPICAL CALENDAR TIME
1. Cybersecurity responsibilities	2–6 hours	1–3 business days
2. Asset & service-provider management	4–12 hours	2–10 business days
3. Default passwords & password policy	2–8 hours	1–5 business days
4. MFA	2–8 hours + user enrollment	1–7 business days
5. Backup & restoration	3–10 hours + restore test	1–10 business days

Planning Estimate for the Implementation of Tier-1 Cybersecurity Practices

Timing assumption: for an SBC with 1–25 employees that already uses commercial email and cloud services. Estimates cover getting to a documented, working, tested practice with evidence, not just switching a feature on. These are DOE SBIR/STTR planning estimates; NIST and CISA don't set these timelines.

Tier 2 Quick Planning Estimate

TIER 2 SUPPLEMENTAL GUIDE

PRACTICE	TYPICAL HANDS-ON EFFORT	TYPICAL CALENDAR TIME
1. Access controls (separate admin accounts and least privilege)	8–24 hours	1–3 business days
2. Secure email	8–24 hours	1–3 business days
3. Strong encryption	12–40 hours	2–5 business days
4. Failed login monitoring	6–24 hours	1–3 business days
5. Incident response plan	8–24 hours	1–3 business days
6. Incident response procedures	12–40 hours	2–5 business days

Planning Estimate for the Implementation of Tier-2 Cybersecurity Practices

Same timing assumption as Tier 1: an SBC with 1–25 employees, existing commercial email and cloud, and a limited number of devices and research systems.

Third-Party Services Commonly Seen in Small R&D Environments

TIER 1 & 2 GUIDES

Common examples

- Microsoft 365 / Microsoft Entra, Google Workspace
- Microsoft Azure, Amazon Web Services (AWS)
- Managed service providers (MSPs)
- Endpoint-management and security products, cloud backup products
- VPN / remote-access services
- Source-code repositories and research SaaS platforms

What your company still must do

- Keep an inventory of the services you use
- Understand the shared-responsibility model
- Restrict administrator access
- Review security settings
- Keep evidence
- Check the service suits the type of federal information you handle
- Company must understand your contract with MSPs.

These services can automate or enforce many practices. They help you do the work; they don't take over your responsibility.

What's in This Video Series

VIDEO SERIES

VIDEO	TOPIC	PRACTICES (EVIDENCE FORM)
1	Cybersecurity Leadership	1.1
2	Assets, Data, and Service Providers	1.2, 1.3
3	Secure Devices and Accounts	1.4, 1.5, 1.6
4	Backups and Restoration	1.7
5	Access Controls	2.1, 2.2
6	Secure Data	2.3, 2.4
7	Unsuccessful-Login Monitoring	2.5
8	Incident Response	2.6, 2.7

Remember These

KEY TAKEAWAYS

1. Describe your environment, data, and providers first
2. A practice counts when it's on, owned, written, known, provable, and current
3. Get Tier 1 approved before you start Tier 2
4. Providers can help, but accountability stays with your company

Up next · Video 1: Cybersecurity Leadership: Your Lead and Program

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