DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

VIDEO 2 OF 8

Know What You Have: Assets, Data, and Providers

TOPIC

Knowing your devices, services, and data, classifying your information, and managing your providers

Practices 1.2 and 1.3 · Tier 1

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

You Can't Protect What You Don't Know You Have

WHY IT MATTERS

01

Devices and systems

Laptops, servers, network gear, lab equipment, and cloud services that handle your work.

02

Your data

Research data, IP, FCI, and CUI, and where each one lives.

03

Your providers

Every company that hosts, manages, or can remotely reach your systems or data.

Manage Organizational Assets and Data

TIER 1 · PRACTICE 1.2

WHAT IT MEANS

Identify, document, and keep up to date a list of the assets that process, store, send, or protect your business information, intellectual property, and CUI.

HOW TO DO IT

1. Identify, classify, and restrict access to your critical intellectual property
2. Inventory data, hardware, software, systems, cloud services, network devices, and research/lab equipment
3. Mark assets authorized or unauthorized; remove, disable, or restrict anything unauthorized
4. Record owner, purpose, location, version, support status, internet exposure, and whether sensitive R&D or CUI is handled
5. Use the list to find your high-value R&D assets and guide risk, setup, incident, and replacement decisions
6. Review it regularly and whenever assets are added, removed, replaced, or changed

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 2.0

What Goes on the Asset Inventory?

PRACTICE 1.2 · THE INVENTORY

01

Computers and network

Laptops, desktops, engineering workstations, servers; routers, firewalls, Wi-Fi, switches, VPN gateways.

02

Research and mobile

Lab equipment that connects to a network or stores data; mobile devices used for work.

03

Storage and software

NAS, external drives, cloud storage, backups; major business and research applications.

04

Cloud and security tools

Microsoft 365, Google Workspace, Azure, AWS, file sharing, code, accounting; endpoint protection, EDR, password manager, scanners, SIEM.

Simple Implementation Steps

PRACTICE 1.2 · BUILDING IT

01

Start with what you have

Purchase records, Microsoft/Google admin consoles, router client lists, cloud subscriptions, lab lists.

02

Use the template

Put it in the DOE SBIR/STTR asset inventory template (Attachment 1) or a similar controlled list.

03

Authorized or not?

Mark each item. Remove, disable, isolate, or investigate anything that shouldn't be there.

04

Flag what's sensitive

Mark assets that store or reach research data, IP, or CUI, and review them first.

05

Review often

Monthly when practical, and right away when new equipment or cloud services arrive.

06

Record exceptions

E.g., an old instrument that can't be patched: note extra protections and a replacement plan.

How Do You Identify and Classify Your Data?

PRACTICE 1.2 · CLASSIFY YOUR DATA

01

Step 1: Is it public?

Public websites, product info, job postings, press releases. If yes, it's generally not FCI or CUI. If no, go to Step 2.

02

Step 2: Is it tied to a federal contract?

Did the Government give it to you, or did you create it doing the contract? If no, it's probably not FCI or CUI, but may still be sensitive.

03

Step 3: Does it need basic protection?

Non-public information provided by or created for the Government under a federal contract may be FCI. Continue to Step 4.

04

Step 4: Does a rule require special protection?

If a law, regulation, or Government-wide policy requires it, it may be CUI. Look for CUI markings, contract terms, or a NARA CUI Registry category.

Data Types at a Glance

PRACTICE 1.2 · CLASSIFY YOUR DATA

TYPE	SIMPLE MEANING	EXAMPLE	GOVERNMENT REFERENCE
Public	Anyone can access it	Public government website	—
Sensitive	Your company believes it needs protection, or another requirement applies	Internal pricing, employee information, proprietary business plans	FTC Protecting Personal Information; NIST SP 800-122
FCI	Non-public information provided by or created for the Government under a federal contract	Non-public contract deliverable	FAR 52.204-21
CUI	Information a law, regulation, or Government-wide policy requires or permits to be safeguarded	Certain controlled technical drawings	NARA CUI Registry; 32 CFR Part 2002; NIST SP 800-171 Rev. 3

Copies, notes, and summaries of CUI are CUI too. Unsure of the category? Ask your contracting officer, prime contractor, security representative, or CUI program contact.

Is It Critical Technology / Intellectual Property?

PRACTICE 1.2 · CRITICAL IP

CATEGORY	WHAT TO WRITE DOWN
Crown jewels	Your most sensitive technology: inventions, source code, formulas, designs, manufacturing processes, algorithms, research, prototypes, technical documents.
Consequence if stolen	Low (limited commercial impact), Moderate (significant competitive disadvantage), High (a competitor could reproduce it), or Critical (could harm U.S. competitiveness, critical infrastructure, defense, or national security).
Who has access	Employees, administrators, contractors, MSPs, manufacturers, suppliers, foreign subsidiaries, research partners, cloud providers.
Where it can leave	Email, USB drives, personal cloud, Git repositories, file sharing, AI apps, remote access, mobile devices, supplier systems.
Planned/implemented controls	How you restrict access, monitor use, stop data leaving, spot unusual behavior, and respond quickly.

Manage Risks from Managed Service Providers (MSPs)

TIER 1 · PRACTICE 1.3

WHAT IT MEANS

Identify and manage the cybersecurity risk from MSPs, MSSPs, and other providers that run, host, monitor, store, process, or remotely access your systems or data.

HOW TO DO IT

1. Keep a provider list showing the services and access each one has
2. Check their security before you choose or renew them, and after big incidents or changes
3. Put security, incident notification, investigation cooperation, and DOE SBIR/STTR requirements in contracts
4. Write down who handles patching, backups, logging, MFA, vulnerabilities, incidents, accounts, and data protection
5. Limit provider access: least privilege, separate admin accounts, and MFA for remote access
6. Review providers at least yearly, and remove access promptly when service ends

More detail: DOE SBIR/STTR Tier 1 Supplemental Guide, section 1.3 (complete the MSP tab of the inventory list)

Tools That Can Help Build Your Inventory

PRACTICE 1.2 & 1.3 · GETTING HELP

SERVICE	HOW IT CAN HELP	KEEP IN MIND
Microsoft 365 / Entra	Users, devices, role assignments, sign-in and security reports help list accounts and devices and review admins.	Won't list lab devices, local network gear, or non-Microsoft apps.
Google Workspace	Admin console users, devices, apps, and security reports show managed accounts, devices, and connected services.	Doesn't replace a full hardware, network, and lab inventory.
AWS / Azure	Resource inventories, tags, IAM, and billing lists identify cloud resources and owners.	Only covers what's in that cloud account.
MSP / endpoint tool	Ask for an export of managed devices, installed software, patch status, and security-tool coverage.	Don't assume it's complete; check it against purchases, network devices, cloud, and lab assets.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Forgotten laptops, accounts, and cloud services become easy ways in.
- Sensitive data goes unprotected because no one knew it was there.
- A breach at your provider can become a breach at your company.
- 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)
1.2 Asset inventory	Asset inventory (template provided by SBIR/STTR Office)
1.2 Managing assets	Process and/or policy for managing assets
1.2 Data classification	Documented data classification process
1.3 Service providers	MSP list found on the inventory list (template provided by SBIR/STTR Office)

Guide estimate: 4–12 hours; 2–10 business days when lab equipment, legacy devices, several cloud accounts, or MSP records must be reconciled.

Remember These

KEY TAKEAWAYS

1. List every device, service, and data type you use
2. Classify your data: Public, Sensitive, FCI, or CUI
3. Know your crown jewels and who can reach them
4. Track every provider, its access, and its contract terms

Up next · Video 3: Secure Devices and Accounts: Passwords and MFA

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