DOE SBIR/STTR SUPPLEMENTAL GUIDE FOR TIER 1 CS PRACTICES

Department of Energy (DOE) Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Supplemental Guide for Tier 1 Cybersecurity Practices

Aligned to NIST SP 800-171 Rev. 3 and CISA Cross-Sector Cybersecurity Performance Goals (CPG) 2.0

Purpose: Turn Tier 1 cybersecurity requirements into practical actions that an SBIR/STTR Small Business Concern (SBC) can complete, document, and show as evidence. The guide also explains where common third-party services can do part of the technical work and where the SBC still owns the responsibility.

Prepared as an awardee-friendly implementation companion • August 2026

Contents

How to Use This Guide 4

Important Scope Note 4

Tier 1 Quick Planning Estimate 4

Third-Party Services Commonly Seen in Small R&D Environments 4

1.0 Cybersecurity Leadership 6

Aligned with CS Practice 1.1 Establish Cybersecurity Responsibilities found on the DOE SBIR/STTR Implementation and Evidence Form 6

What the SBC Should Do 6

Can a third-party service provider help? 6

2.0 Manage Organizational Assets, Data, and Service Providers 7

Aligned with CS Practice 1.2 Managing Organization Assets and 1.3 Manage Risks from Managed Service Providers found on the DOE SBIR/STTR Implementation and Evidence Form 7

1.2 Managing Organizational Assets and Data 7

What Goes on the Asset Inventory? 7

How do you identify and classify data? 8

Simple Implementation Steps 8

3.0 Secure Devices and Accounts 12

Aligned with CS Practice 1.4 Change or Disable Default Passwords and Accounts, 1.5 Establish and Enforce Minimum Password Strength, and 1.6 Implement Multi-Factor Authentication found on the DOE SBIR/STTR Implementation and Evidence Form 12

1.4 Change or Disable Default Passwords and Accounts 12

DOE Requirement: Change or disable manufacturer/vendor default passwords, accounts, and authenticators before systems are placed into production or connected to SBC networks. Before a new device, application, research instrument, or cloud service is placed into normal use, change manufacturer/vendor default credentials and disable unnecessary default, guest, demo, or test accounts. 12

Implementation Steps 12

Where to Check 13

1.5 Establish and Enforce Strong Password Management 13

DOE Requirement: Establish and enforce a password policy that makes passwords difficult to guess or crack. Use long, unique passwords/passphrases; block weak or compromised passwords where the platform supports it; do not force routine password changes without a reason; and use a business password manager when practical. 13

Recommended SBC Baseline 14

1.6 Implement Multi-Factor Authentication (MFA) 14

Microsoft 365 / Microsoft Entra — Use Current Microsoft Instructions 15

Google Workspace — Use Current Google Instructions 15

Table of Contents

4.0 — Maintain Backups and Restoration Ability 16

Aligned with CS Practice 1.7 Maintain System Backups & Restoration Ability found on the DOE SBIR/STTR Implementation and Evidence Form 16

Implementation Steps 16

Common Cloud Options 17

What Counts as Good Evidence? 17

Vendor-Specific Guidance Policy 17

Source and Alignment Notes 18

Use of CISA CPG 2.0 18

Implementation-Time Disclaimer 18

How to Use This Guide

Tier 1 focuses on four foundational areas: 1.0 Cybersecurity Leadership, 2.0 Manage Organizational Assets and Service Providers, 3.0 Secure Devices and Accounts, and 4.0 Maintain Backups & Restoration Ability. These are the same core areas identified in the source Tier 1 guide, but the instructions below are reorganized for an SBC that may have a small staff, limited IT support, and extensive use of cloud or managed services.

> **Please Note:** A third-party service can provide a security feature, but SBC must make sure the feature is turned on, configured correctly, applied to the right users/systems, reviewed, and documented. Outsourcing IT does not outsource accountability. Vendor-specific steps below are based on vendor-published documentation. Cloud interfaces and licensing change frequently. Before implementation, SBC should use the linked vendor documentation and verify that the feature is available in its current subscription or service tier.

What "fully implemented" should mean for an SBC

- The technical setting or process is enabled and operating on the systems within scope.
- Responsibility is assigned to an employee, owner, IT administrator, MSP, or MSSP.
- The SBC has a short-written policy, procedure, or configuration record describing the practice.
- Personnel who must follow the practice know what is expected.
- If needed, SBC can provide reasonable evidence such as screenshots, exported settings, logs, reports, tickets, policies, or test results.
- The SBC reviews and updates (as needed) the practice periodically and after significant system, personnel, or service changes.
- Security practices are sufficient at protecting CUI, FCI, and sensitive information from unauthorized disclosure.

Important Scope Note

NIST SP 800-171 Rev. 3 applies when CUI is processed, stored, transmitted, or protected by a nonfederal system. For an SBIR/STTR applicant or awardee that does not handle CUI, these practices still provide a strong baseline for protecting federally funded research, intellectual property, proposal information, business information, and other sensitive data. If CUI is involved, the SBC must also confirm that its contractual requirements, system boundary, cloud/service-provider use, and any required federal authorizations are satisfied.

Tier 1 Quick Planning Estimate

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

Timing assumption: These estimates are specifically tailored to a DOE SBIR/STTR R&D Small Business Concern (SBC) with 1–25 employees. They estimate the total labor effort needed to reach a documented, operational, tested, and evidence-supported implementation—not merely the time needed to enable a technical feature. Assumptions include an existing commercial email/cloud environment and a limited number of endpoints and research systems. These are DOE SBIR/STTR planning estimates; NIST and CISA do not prescribe these implementation durations.

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

Common examples include Microsoft 365/Microsoft Entra, Google Workspace, Microsoft Azure, Amazon Web Services (AWS), managed service providers (MSPs), endpoint-management/security products, cloud backup

products, virtual private network (VPN)/remote-access services, source-code repositories, and research software as a service (SaaS) platform. These services can automate or enforce many Tier 1 practices. SBC should still maintain an inventory of the services, understand the shared-responsibility model, restrict administrator access, review security settings, retain evidence, and verify that the service is appropriate for the type of federal information being handled.

Acronyms

Acronym / Abbreviation	Meaning
AWS	Amazon Web Services
CPG	Cybersecurity Performance Goal
CUI	Controlled Unclassified Information
DOE	U.S. Department of Energy
EDR	Endpoint Detection and Response
FCI	Federal Contract Information
FIDO2	Fast Identity Online 2
IAM	Identity and Access Management
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NAS	Network-Attached Storage
NIST	National Institute of Standards and Technology
PI	Principal Investigator
R&D	Research and Development
SaaS	Software as a Service
SBC	Small Business Concern
SBIR	Small Business Innovation Research
SIEM	Security Information and Event Management
SSP	System Security Plan
STTR	Small Business Technology Transfer
2SV	2-Step Verification
VPN	Virtual Private Network

1.0 Cybersecurity Leadership

Aligned with CS Practice 1.1 Establish Cybersecurity Responsibilities found on the DOE SBIR/STTR Implementation and Evidence Form

1.1 Establish Cybersecurity Responsibilities

DOE Requirement: Name one person who is accountable for cybersecurity. In a very small company, this may be the owner, PI, operations lead, or an IT/security employee. An MSP or consultant may perform technical work, but an SBC employee or authorized leader should remain accountable for oversight, decisions, risk acceptance, resources, and evidence.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Planning; Assessment, Authorization and Monitoring; Risk Assessment; System and Services Acquisition; Supply Chain Risk Management families. Use these requirements to document the system, assess risk, evaluate controls, and manage external providers.	Governance and accountability outcomes in CPG 2.0: assign cybersecurity responsibility, integrate cyber risk into business decisions, and maintain measurable foundational protections.

What the SBC Should Do

1. Appoint a cybersecurity lead in writing. Record the person's name, role, authority, backup contact, and the date assigned.
2. Define what the lead is responsible for such as, but not limited to: cybersecurity plan, asset inventory, account and access reviews, risk assessments, vulnerability tracking, backups, service-provider oversight, insider threat management, incident readiness, and evidence collection.
3. Identify the systems and data the SBC is protecting, including research data, intellectual property, proposal/award information, business data, and CUI when applicable. See section 1.2 Managing Organizational Assets for more information on how to identify and classify data.
4. Create or maintain a simple cybersecurity plan describing the environment and how required practices are implemented.
5. Set a review schedule. At minimum, review the program annually and after a major technology change, security incident, new cloud provider, merger, office/lab move, or material change in federal requirements.
6. Periodically verify controls through an independent assessment and track identified issues to closure.
7. Track open cybersecurity gaps in a corrective-action list with an owner and target completion date.

Conduct Risk Assessments

- Conduct periodic security assessments to verify that controls are implemented and operating effectively.
- Perform penetration testing where warranted by risk.
- Track vulnerabilities and findings to closure using a remediation tracker (e.g. plan of action and milestones).

Conduct Cybersecurity Awareness Training

- Train employees to protect against credential theft.
- Employees should also be trained to recognize insider threats, phishing, and data-handling risks.
- Test CS awareness of personnel by periodically conducting exercises, such as phishing.

Can a third-party service provider help?

Common service/provider	Can it help?	SBC- Suggested Action	Important limitation

Managed Service Provider / Managed Security Service Provider MSSP	Yes — often substantially.	Use the provider for patching, endpoint management, account administration, log review, backups, vulnerability scanning, or technical support. Put responsibilities in the contract/SOW.	The SBC should not make the MSP the only owner of federal compliance or risk acceptance.
Microsoft 365 / Entra	Yes.	Use admin roles, security reports, multifactor authentication (MFA), access controls, and audit capabilities to support the lead's work.	Features vary by license; the SBC must assign and review roles.
Google Workspace	Yes.	Use administrator roles, 2-Step Verification, user/security reporting, and organizational settings.	The SBC must configure and enforce settings; defaults alone may not meet the intended outcome.
AWS / Azure / other cloud	Yes.	Use identity access management (IAM), logging, configuration, backup, and security-management services; assign named owners and review permissions.	Cloud provider security does not automatically secure the SBC's accounts, data, or configurations.

Evidence Required SBC's CS personnel list. (Attachment 1)	Approximate implementation time: 2–6 hours for a small SBC if roles and systems are already known; 1–3 business days if leadership approval or an MSP responsibility review is needed.

2.0 Manage Organizational Assets, Data, and Service Providers

Aligned with CS Practice 1.2 Managing Organization Assets and 1.3 Manage Risks from Managed Service Providers found on the DOE SBIR/STTR Implementation and Evidence Form

1.2 Managing Organizational Assets and Data

DOE Requirement: Keep one current list of the technology and services used to run the business and perform the R&D. If the SBC does not know what it owns, uses, connects, or allows to access research data, it cannot reliably protect.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Configuration Management (system component inventory and controlled configuration); Risk Assessment; System and Services Acquisition; Supply Chain Risk Management; Access Control. Inventory and risk-management activities should cover components and external services within the applicable system boundary.	Asset visibility, risk management, governance, and third-party/supply-chain outcomes in CPG 2.0. The goal is to know what is present, what is authorized, who manages it, and what risk it creates.

What Goes on the Asset Inventory?

Identify the business' computers, servers, cloud services, networks, and other technology used to process, store, transmit, or protect business information, intellectual property, FCI, and CUI.

- Computers and workstations: laptops, desktops, engineering workstations, servers.
- Network equipment: routers, firewalls, wireless access points, switches, VPN gateways.
- Research/lab equipment that connects to a network or stores/transfers data.
- Mobile devices used for SBC work, when permitted.
- Storage: NAS, external drives, cloud storage, backup repositories.
- Software and major business/research applications.
- Cloud/SaaS services: Microsoft 365, Google Workspace, Azure, AWS, file-sharing, source-code, project-management, accounting, and research platforms.

- Security tools: endpoint protection, endpoint detection and response (EDR), password manager, vulnerability scanner, logging/security information and event management (SIEM).

Simple Implementation Steps

8. Start with what you already have: purchase records, Microsoft/Google admin consoles, router/firewall client lists, endpoint-management consoles, cloud subscriptions, and lab equipment lists.
9. Put the information into the DOE/SBIR/STTR asset inventory template (attachment 1) or another controlled inventory that contains the needed fields.
10. Mark each asset/service as authorized or unauthorized. Remove, disable, isolate, or investigate anything that should not be present.
11. Identify which assets store or access research data, intellectual property, or CUI. Give these assets higher review priority.
12. Review the inventory at least monthly for additions/removals when practical, and immediately when new equipment or cloud services are introduced.
13. Record exceptions, such as a legacy research instrument that cannot be patched or cannot support modern authentication. Document compensating controls and a replacement/upgrade plan.

How do you identify and classify your data?

You do not need to be a cybersecurity expert to identify the information your company handles. Start by asking where the information came from, why you have it, and whether the Government requires it to be protected?

Follow the steps to identify and classify data:

Step 1 — Ask: Is this public information?

Examples might include:

- Information posted on a public government website
- Public product information
- Public job postings
- Public press releases
- Information anyone can legally access
    - If YES: It is generally not FCI or CUI.
- If NO: Continue to Step 2.

Step 2 — Ask: Does this information relate to a Federal Government contract? Did the Government give us this information, or did we create it while performing a Federal Government contract?"

Examples might include:

- Contract-related documents
- Project schedules
- Government-provided information
- Reports prepared for the Government
- Deliverables
- Non-public contract information

- **If NO:** It is probably not FCI or CUI based on that contract. However, it may still be sensitive business information and may need protection for other reasons.
- **If YES:** Continue to Step 3.

Step 3 — Ask: Does the information simply need basic protection because it relates to the Federal contract?

This may be FCI. A simple way to think about FCI is: Non-public information provided by or created for the Government while performing a Federal Contract.

Examples could include:

- Non-public contract information
- Project schedules
- Contract deliverables
- Internal contract communications
- Certain reports created for the Government
- Some information is excluded from the FCI definition, such as information the Government has made public and simple transactional information needed to process payments.
    - **If the information fits the FCI definition and no additional CUI protection applies, treat it as FCI.**
- Then continue to Step 4 because some contract information may also qualify as CUI.

Step 4 — Ask: Does the information require special protection under a law, regulation, or Government-wide policy?

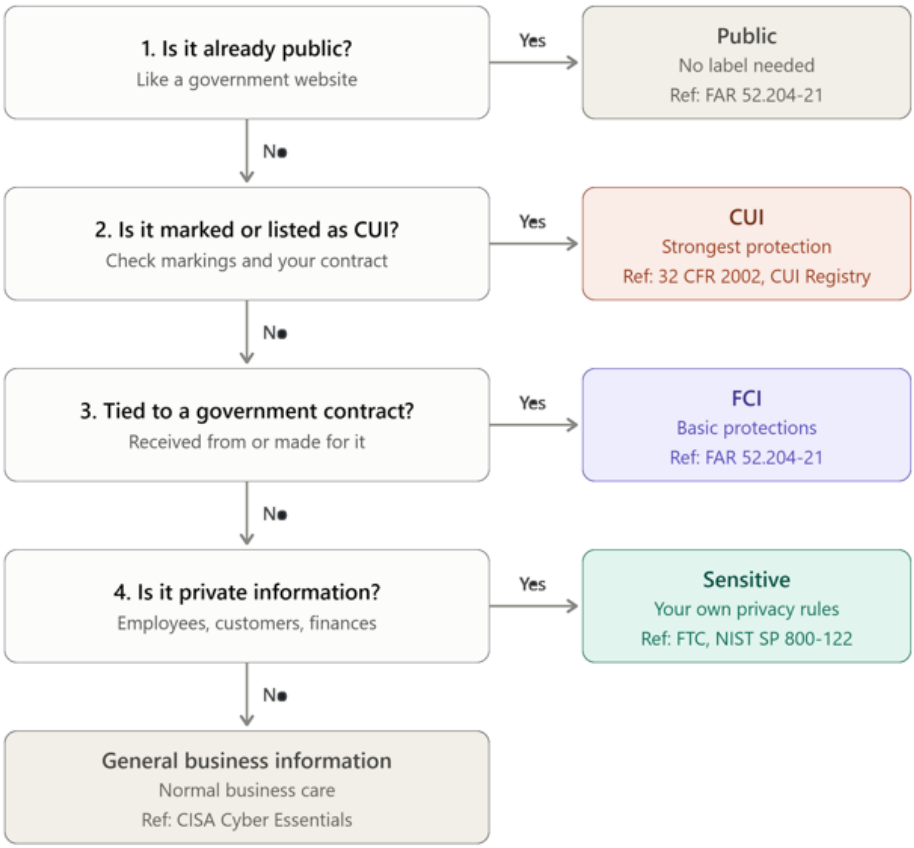
- If YES, the information may be Controlled Unclassified Information (CUI).
- Do not decide that something is CUI simply because it looks sensitive.

Look for:

- CUI markings on the document.
- CUI requirements in the contract.
- Instructions from the Government customer.
- A CUI category listed in the National Archives CUI Registry.
- A law or regulation requiring information to be protected.
- Distribution statements or other Government handling instructions.
- Examples of information that can qualify as CUI include certain:
    - Engineering drawings
    - Technical specifications
    - Technical reports
    - Research and engineering information
    - Export-controlled information
    - Copies, notes, and summaries of CUI are classified as CUI as well.
    - Privacy information
    - Critical infrastructure information
    - Law enforcement information
    - For example, certain military or space-related technical information may qualify as Controlled Technical Information (CTI), which is a category of CUI.

***Note:** If information is believed to be CUI but cannot determine the category or authority, please ask your government contracting officer, prime contractor, security representative, or CUI program contact for clarification.

Type	*Simple Meaning*	*Example*
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
FCI	Non-public information provided by or created for the Government under a Federal contract	Non-public contract deliverable
CUI	Government-related information that a law, regulation, or Government-wide policy requires or permits to have safeguarding or dissemination controls	Certain controlled technical drawings



GOVERNMENT REFERENCES:

DATA CLASSIFICATION	GOVERNMENT REFERENCES

• **FCI**	• FAR 52.204-21, definition and 15 safeguards
• **CUI**	• NARA CUI Registry, official list of CUI Categories • 32 CFR Part 2002, the federal CUI regulation • NIST 800-171 rev3, how to protect CUI
• **CUI (DOD)**	• DOD (DOW) CUI Program and DFARS 252.204-7012
• **SENSITIVE**	• FTC, Protecting Personal Information: Guide for Business
	• NIST SP-800-122, Protecting Personal Information (PII)
• **GENERAL**	• CISA Cyber Essentials, starter kit for small organizations

Is it Critical Technology / Intellectual Property?

Use this impact worksheet to think through what SBC's most important technology is, what would happen if it were stolen, who can reach it, and how it could leave the organization.

Category	SBC Notes
Crown jewels	List the company's most sensitive technology, inventions, source code, formulas, designs, manufacturing processes, algorithms, research, prototypes, and technical documentation.
Consequence if stolen	Rate the impact: Low (limited commercial impact), Moderate (significant competitive disadvantage), High (could allow a competitor to reproduce the technology), or Critical (could materially harm U.S. economic competitiveness, critical infrastructure, defense, or national security).
Who has access	List categories with access, e.g., employees, administrators, contractors, MSPs, manufacturers, suppliers, foreign subsidiaries, research partners, and cloud providers.
Where it can leave	List the pathways information could leave the organization, e.g., email, USB, personal cloud, Git repositories, file sharing, AI applications, remote access, mobile devices, and supplier systems.
Planned/implemented controls	Summarize the controls in place or planned to restrict access, monitor use, control exfiltration, detect abnormal behavior, and enable a rapid response for this category of IP.

1.3 Manage Risks from Managed Service Providers (MSPs)

DOE Requirement: Identify and manage cybersecurity risk from MSPs/Managed Security Service Providers (MSSPs) and other providers that administer, host, monitor, store, process, or remotely access SBC systems or data.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Supply Chain Risk Management; Access Control; System and Services Acquisition. Use these requirements to assess provider risk, document shared responsibilities, and limit provider access.	Third-party/supply-chain risk outcomes in CPG 2.0: know which providers can reach SBC systems/data and manage that risk deliberately.

Complete the MSP tab found in the inventory list (Attachment 2). Include any provider that hosts, stores, processes, administers, monitors, backs up, or has remote access to SBC critical systems, sensitive data, FCI, or CUI.

- Before selection or renewal, review the provider's security capabilities, incident history where available, authentication options, encryption, logging, backup/recovery, and support model.

- Document the shared responsibility: who patches, backs up, monitors logs, creates accounts, removes accounts, manages MFA, handles incidents, and retains evidence. Keep in mind what service are used in support of the SBIR/STTR research and development efforts.
- Require least-privilege access and separate administrative accounts for provider personnel.
- Require MFA for provider remote/admin access whenever supported.
- Track provider performance and remove provider accounts and credentials promptly when the service or contract ends.

Common service/provider	Can it help?	SBC-friendly enablement	Important limitation
Microsoft 365 / Entra	Yes.	Use Users, Devices, Role assignments, sign-in/security reports, and device-management features (where licensed) to help identify users/devices and review administrators.	It will not inventory every lab device, local network appliance, or non-Microsoft SaaS product.
Google Workspace	Yes.	Use Admin console users, devices, apps, security reports, and admin roles to identify managed accounts/devices and connected services.	It will not replace a complete hardware/network/research-equipment inventory.
AWS / Azure	Yes.	Use resource inventories, tags, IAM, cloud asset/configuration tools, and billing/subscription lists to identify cloud resources and owners.	Cloud inventory only covers resources visible in that cloud account/subscription.
MSP / endpoint-management tool	Yes.	Ask the MSP to export managed endpoints, installed software, patch status, and security-tool coverage. Reconcile that export to the SBC inventory.	Do not assume the MSP list is complete; independently reconcile it to purchases, network devices, cloud services, and lab assets.

Evidence Required SBC's MSP list found on the inventory list (Attachment 2).	Approximate implementation time: 4–12 hours for a 1–25 user cloud-first SBC. Allow 2–10 business days when lab equipment, legacy devices, multiple cloud accounts, or MSP records must be reconciled.

3.0 Secure Devices and Accounts

Aligned with CS Practice 1.4 Change or Disable Default Passwords and Accounts, 1.5 Establish and Enforce Minimum Password Strength, and 1.6 Implement Multi-Factor Authentication found on the DOE SBIR/STTR Implementation and Evidence Form

1.4 Change or Disable Default Passwords and Accounts

DOE Requirement: Change or disable manufacturer/vendor default passwords, accounts, and authenticators before systems are placed into production or connected to SBC networks. Before a new device, application, research instrument, or cloud service is placed into normal use, change manufacturer/vendor default credentials and disable unnecessary default, guest, demo, or test accounts.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Identification and Authentication; Configuration Management; Access Control. The intended outcome is to prevent use of known/default authenticators and limit accounts to authorized users and purposes.	Credential security, secure configuration, and account-protection outcomes in CPG 2.0.

Implementation Steps

14. Update the device/application first when the vendor recommends doing so.
15. Perform vulnerability scanning on the device to identify and patch weaknesses. (conduct periodically thereafter).

16. Perform periodic vulnerability scanning to identify weakness that patching alone may not catch.
17. Sign in using the initial/default administrator credential.
18. Create a named SBC administrator account where supported.
19. Set a unique strong password or passphrase; store it in the approved business password manager if one is used.
20. Disable or remove unnecessary default/guest/test accounts.
21. Turn on MFA for administrator access where the product supports it. Information regarding MFA can be found in DOE SBIR/STTR Supplemental Guide for Tier 1 CS Practices, section 1.6 Implement Multi-Factor Authentication.
22. Verify the password change before use in production.
23. Record the completion date in the asset inventory or deployment checklist.
24. If a legacy device cannot change a default credential, isolate/restrict access, monitor it, document the limitation, and plan replacement or upgrade.

Where to Check

Common service/provider	Can it help?	SBC-friendly enablement	Important limitation
Microsoft 365 / Entra	Yes.	Review active users and administrator role assignments; remove unneeded accounts; require MFA for admins. Cloud tenants generally do not rely on a shared manufacturer default password, but initial/admin accounts still require secure configuration.	Do not share Global Administrator credentials.
Google Workspace	Yes.	Review users/admin roles; remove unused accounts; enforce 2-Step Verification. Google administrator accounts should be individually assigned.	Avoid shared administrator accounts.
Routers / firewalls / Wi-Fi / NAS	Usually.	Open the vendor's management console, change the factory admin password, disable remote administration unless required, and disable unused accounts/services.	Exact menu names differ by manufacturer.
Research/IoT equipment	Sometimes.	Use the vendor administration interface/manual to change credentials and disable unused services/accounts.	Older equipment may not support modern controls; document compensating controls.

Evidence Required: SBC's password policy and/or process that addresses changing or disabling default passwords and accounts.	Approximate implementation time: 5–20 minutes per normal device/service; 2–8 total hours for a small environment. Legacy or vendor-managed research equipment may require several business days.

1.5 Establish and Enforce Strong Password Management

DOE Requirement: Establish and enforce a password policy that makes passwords difficult to guess or crack. Use long, unique passwords/passphrases; block weak or compromised passwords where the platform supports it; do not force routine password changes without a reason; and use a business password manager when practical.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Identification and Authentication, especially password/authenticator management; Access Control. NIST Rev. 3 emphasizes managed authenticators and stronger authentication practices rather than relying on frequent arbitrary password rotation.	Credential security and identity-protection outcomes in CPG 2.0.

Recommended SBC Baseline

- Require at least 16 characters whenever the system supports it; favor memorable passphrases.
- Require a different password for each business account; never reuse a business password on a personal account.
- Block common, easily guessed, or known-compromised passwords where the platform supports password protection.
- Do not require 30/60/90-day password changes solely because time passed. Change a password when compromise is suspected/confirmed, a credential is exposed, or an account recovery/reset is required.
- Use an approved password manager for business credentials when feasible.
- For systems that cannot support the baseline, document the limitation and add controls such as MFA, network restriction, logging, or accelerated replacement.

Common service/provider	Can it help?	SBC-friendly enablement	Important limitation
Microsoft 365 / Entra	Yes.	Use Microsoft Entra password-protection capabilities where available; keep password expiration disabled unless a specific requirement says otherwise; combine passwords with MFA/security defaults or Conditional Access.	Some advanced controls require additional licensing.
Google Workspace	Yes.	Use Admin console password-management and account-security settings; enforce 2-Step Verification; reset credentials when compromise is suspected.	Exact password controls vary by Workspace edition.
Password manager	Yes.	Deploy an organization-approved vault; require unique generated passwords; protect the vault with MFA; define recovery and offboarding procedures.	A password manager is a supporting control, not a replacement for MFA or access reviews.
MSP	Yes.	Have the MSP configure tenant/device password settings and provide an export/screenshot showing the policy.	SBC should approve the policy and retain evidence.

Evidence Required: SBC's password-management policy and/or process.	Approximate implementation time 1–3 hours to establish policy and configure a cloud-first SBC; 1–5 business days if multiple applications must be checked individually.

1.6 Implement Multi-Factor Authentication (MFA)

DOE Requirement: Require MFA for access to SBC business/work systems, using the strongest available method. A password by itself should not be enough to access important SBC systems. Require a second factor for employees, administrators, remote access, cloud services, email, collaboration/file sharing, and systems that hold federally funded research, IP, or CUI.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
Identification and Authentication and Access Control. Apply MFA to privileged and non-privileged access as required by the applicable NIST SP 800-171 Rev. 3 authentication requirements and system scope.	Identity and access management outcomes in CPG 2.0, including strong MFA and preference for phishing-resistant authentication for higher-risk access.

Preferred method: Use phishing-resistant MFA (for example, Fast IDentity Online FIDO2 security keys or passkeys) when feasible, especially for administrator and other high-impact accounts. App-based methods are generally preferable to short message service (SMS) when phishing-resistant methods are not available.

Microsoft 365 / Microsoft Entra — Use Current Microsoft Instructions

1. SBC should configure Microsoft 365 / Microsoft Entra so required accounts are protected by MFA. Do not rely on a fixed menu path in this DOE/SBIR/STTR guide. Microsoft changes administrative portals, licensing, authentication methods, and recommended configurations over time.

   Current Microsoft guidance identifies Security Defaults as the baseline option available through Microsoft Entra ID Free and Conditional Access as the more configurable option for eligible Microsoft Entra ID P1/P2 environments. Microsoft identifies legacy per-user MFA as not recommended.

   Implementation rule: The SBC should open Microsoft's current official MFA documentation at the time of implementation, determine which Microsoft-supported method applies to its tenant and license, follow Microsoft's current configuration instructions, test the configuration, and retain evidence showing the resulting setting.

   Evidence to retain: Microsoft-generated configuration screenshot/export, applicable Conditional Access or Security Defaults evidence, user/authentication registration evidence where available, administrator protection evidence, test/review date, and documented exceptions.

   Vendor-controlled instructions:
   Microsoft — Set up multifactor authentication for Microsoft 365 https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

Google Workspace — Use Current Google Instructions

2. SBC action: Configure Google Workspace so required users and administrators use 2-Step Verification (2SV). Do not rely on a fixed Google Admin console menu path in this DOE/SBIR/STTR guide because Google can change its interface, available methods, and enforcement options.

   Google's current administrator guidance recommends enforcing 2SV for administrators and users who handle important business information. Google identifies security keys as its strongest 2SV method and discourages text-message verification. Google also provides passkey capabilities using phishing-resistant technology.

   Implementation rule: The SBC should open Google's current official administrator documentation at the time of implementation, follow the current deployment/enforcement instructions applicable to its Workspace edition, enroll users safely, test access, and retain evidence of enforcement.

   Evidence to retain: Google Admin configuration screenshot/export, 2SV enrollment/enforcement evidence, administrator protection evidence, test/review date, and documented exceptions.

   Vendor-controlled instructions:
   Google Workspace Admin Help — Protect your business with 2-Step Verification
   https://support.google.com/a/answer/175197

Common service/provider	Can it help?	SBC-friendly enablement	Important limitation
Microsoft 365 / Entra	Yes — strongly.	Security Defaults or Conditional Access can enforce MFA. Microsoft also supports phishing-resistant authentication methods for privileged roles.	Conditional Access requires eligible licensing; test policies to avoid lockouts.

Google Workspace	Yes — strongly.	Admin console can allow and enforce 2-Step Verification; use security keys/passkeys where feasible.	Enroll admins/users before enforcement and maintain recovery procedures.
AWS	Yes.	Use IAM/IAM Identity Center and require MFA for administrative and human access; protect the root user with strong MFA and avoid routine root use.	The SBC must configure identities and policies; AWS does not automatically enforce the SBC's desired access model.
VPN / remote access / MSP portal	Usually.	Enable the product's MFA/SSO setting; if possible federate access to the SBC's Microsoft/Google identity provider so one policy can enforce MFA.	Verify every remote/admin path is covered, including break-glass or vendor accounts.

Suggested evidence SBC's policy and/or process for enforcing MFA to include documented exceptions and recovery procedure.	Approximate implementation time 2–4 hours for a small cloud tenant plus user enrollment; typically 1–7 business days to enroll everyone safely. Multiple VPNs, SaaS tools, or legacy systems can extend the schedule.

4.0 — Maintain Backups and Restoration Ability

Aligned with CS Practice 1.7 Maintain System Backups & Restoration Ability found on the DOE SBIR/STTR Implementation and Evidence Form

1.7 Maintain System Backups & Restoration Ability

DOE Requirement: Back up the information and configurations needed to restore R&D operations after cyberattacks, such as, a ransomware incident, hardware failure or accidental loss. Make reliable copies of the systems and information the SBC needs to continue research and business operations, protect those copies from unauthorized access or deletion, and prove through periodic testing that the SBC can restore usable data after ransomware, accidental deletion, equipment failure, corruption or another disruptive event.

NIST SP 800-171 Rev. 3 alignment	CISA CPG 2.0 alignment
System and Information Integrity; Contingency/recovery-related protections reflected across applicable NIST requirements and the organization's documented security plan. For CUI systems, backup copies and recovery processes remain within the security boundary and must be protected commensurate with the information they contain.	Resilience and recovery outcomes in CPG 2.0: maintain protected backups and verify restoration so ransomware, hardware failure, or accidental loss does not permanently stop operations.

Implementation Steps

1. Use the asset inventory to identify what must be backed up: research data, IP, source code, configuration files, critical business records, servers, cloud workloads, and CUI where applicable.
2. Define a backup schedule based on how much data the SBC can afford to lose. Critical research data may need daily or more frequent protection.
3. Keep at least one backup copy logically or physically separated from the production environment. Where available, use immutable or deletion-protected backup features.
4. Restrict backup administration to authorized personnel and require MFA for backup administrators.
5. Encrypt backup data when appropriate and ensure keys/recovery credentials are protected.
6. Perform a restore test on a representative file/system. Confirm the restored data is complete, readable, accurate, and usable.
7. Document the test date, person performing the test, item restored, result, problems found, and corrective action.
8. Review backup and restoration procedures at least annually and after significant changes.

Common Cloud Options

Common service/provider	Can it help?	SBC-friendly enablement	Important limitation
Microsoft 365	Yes.	Use Microsoft 365 retention/recovery capabilities and, where selected, Microsoft 365 Backup or an approved third-party backup service. Configure protected users/sites and retention according to business needs.	Native retention/recycle capabilities and a dedicated backup strategy are not always the same thing. Confirm recovery objectives and test restoration.
Google Workspace	Partly / Yes with add-ons or third party.	Use native recovery/retention features appropriate to the Workspace edition and, when needed, a dedicated Workspace backup product. Test restore of representative files/mail.	Do not assume SaaS availability equals a complete backup that meets the SBC's recovery needs.
AWS	Yes.	Use AWS Backup to create backup plans, schedules, retention, vault controls, and protected copies; restrict vault access and test recovery.	The customer remains responsible for selecting resources, schedules, permissions, retention, and restore testing.
Azure	Yes.	Use Azure Backup/Recovery Services or other approved backup services; configure policies, protected items, retention, and restore testing.	Verify the service covers each workload and data type.
MSP / backup vendor	Yes.	Require the provider to document backup scope, frequency, retention, separation/immutability, monitoring, failed-job handling, and restore testing.	SBC should receive evidence and participate in or independently verify restore tests.

Suggested evidence SBC's backup and restore policy/process.	Approximate implementation time 3–10 hours for initial configuration and a representative restore test; typically 1–10 business days depending on data volume, first backup completion, and restore-test scheduling.

What Counts as Good Evidence?

Evidence should show both the written expectation and the actual technical setting, however, a policy by itself is acceptable evidence for SBIR/STTR Office to show that the practice has been implemented.

> **Evidence tip:** Redact passwords, private keys, recovery codes, secrets, tokens, and unnecessary personal information from submitted evidence.

Vendor-Specific Guidance Policy

Vendor-specific configuration guidance in this document is intentionally limited to the security outcome the SBC should achieve. When a vendor provides current official implementation instructions, those vendor instructions are the controlling technical reference for menu paths, prerequisites, licensing, supported authentication methods, configuration steps, and product-specific limitations. The SBC should use the vendor's current official documentation at the time of implementation, because cloud services and administrative interfaces change frequently. DOE/SBIR/STTR planning estimates and evidence recommendations in this guide are not vendor requirements.

Source and Alignment Notes

This guide is based on the DOE SBIR/STTR Cybersecurity Implementation and Evidence Form and expands its four core implementation areas into awardee-friendly technical steps. NIST and CISA sources establish cybersecurity outcomes and federal alignment. Vendor-specific implementation references are limited to current official vendor documentation; third-party blogs, community posts, and unofficial setup instructions should not be used as the authoritative configuration source.

- NIST SP 800-171 Rev. 3 — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (May 2024)
- NIST SP 800-171A Rev. 3 — Assessing Security Requirements for CUI (May 2024)
- NIST SP 1318 — NIST SP 800-171 Rev. 3 Small Business Primer (August 2025)
- CISA — Cross-Sector Cybersecurity Performance Goals / CPG 2.0
- CISA announcement — Cybersecurity Performance Goals 2.0 (December 2025)
- Microsoft — Set up multifactor authentication for Microsoft 365
- Microsoft — Configure Security Defaults for Microsoft Entra ID
- Microsoft — Administrator roles in Microsoft 365
- Microsoft — Microsoft 365 Backup setup
- Google Workspace — Protect your business with 2-Step Verification
- Google Workspace — Allow users to use passkeys / skip passwords
- AWS — AWS Backup Developer Guide
- AWS — Security best practices for backups

Use of CISA CPG 2.0

CISA released CPG 2.0 in December 2025 and describes the goals as measurable, foundational, outcome-oriented cybersecurity actions aligned with the current NIST Cybersecurity Framework. Because DOE SBIR/STTR tier terminology may be organized differently from CISA's current goal numbering, this guide maps each Tier 1 practice to the applicable CPG 2.0 outcome area rather than treating older CPG numbers as current 2.0 identifiers.

Implementation-Time Disclaimer

The time estimates in this guide are planning estimates, not NIST or CISA requirements. They assume a small organization with a limited number of users and systems. Actual time depends on environment size, licensing, legacy equipment, user enrollment, vendor support, data volume, and whether CUI or other contract-specific requirements apply.