Department of Energy (DOE) Small Business Innovative Research and Small Business Technology Transfer (SBIR/STTR) Tiers 1 and 2 Cybersecurity Implementation & Evidence Form

How to Use This Form

- Complete the small business award information and environment profile.
- For each DOE requirement, read the implementation guidance.
- If additional implementation information is needed, please refer to the DOE SBIR/STTR - Supplemental Guide for Tier 1 Cybersecurity Practices.
- Attach or identify objective evidence. A documented policy or operational evidence may be sufficient to prove compliance. Please refer to each evidence section in each requirement.
- Tier 1 cybersecurity practices must be submitted and approved by the SBIR/STTR Office before the applicant/awardee can begin implementing Tier 2 cybersecurity practices.

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, the 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.

Framework Alignment Note

DOE cybersecurity tier requirements are the controlling program requirements represented by this form. The Cybersecurity Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs version 2.0 and National Institute of Standards & Technology Special Publication (SP) 800-171 Revision 3 (NIST SP 800-171r3) references are included to clarify implementation outcomes and evidence. NIST SP 800-171r3 applies to nonfederal system components that process, store, transmit, or protect Controlled Unclassified Information (CUI). CISA CPG version 2.0 reorganized and renumbered several goals. This revision uses version 2.0 identifiers rather than the older CPG numbering. For example, Establish Cybersecurity Responsibilities is now 1.B. **Scope note:** NIST SP 800-171 Rev. 3 applies to nonfederal system components that process, store, transmit, 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.

1. Small Business and Award Information

Small Business Concern (SBC) (Legal Name)	Click or type here.
Current DOE SBIR/STTR Award Number	Click or type here.
Phase / Release	Click or type here.
Principal Investigator	Click or type here.
Cybersecurity Lead	Click or type here.
Date Completed / Last Updated	Click or type here.

2. Small Business Environment and Scope

Small Business Environment	Where is the work being performed? How is the work performed? Describe the business' computers, servers, cloud services, networks, and other technology used to process, store, transmit, or protect business information, intellectual property, and CUI. This is not limited to just computers or a physical office.
Protected Information	Identify data types used in the business environment, such as, federal funded research, intellectual property source code, engineering/scientific data, business information, sensitive information, federal contract information, and controlled unclassified information when applicable. If unsure on how to identify protected information, then refer to the Supplemental Guide for Tier 1 Cybersecurity Practices.
Managed / Cloud Services	List MSP/MSSP, email, cloud, collaboration, backup, security, hosting, or other providers that administer, host, store, process, monitor, or remotely access SBC systems/data. This includes cloud/services for emails/collaboration, cloud file storage/infrastructure, source-code, back-ups/recovery, business applications, project management, communication, AI services and research/engineering platform.

Example:

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 (i.e. pricing, financial information, business strategies), prototype/test information, and personnel information.
Managed / Cloud Services	Our cloud infrastructure consists of AWS, Google Cloud, and Microsoft Azure. We use Microsoft 365 and Google Workspace to send emails and collaborate. We store our files in Google Drive and OneDrive. We use GitHub to store our source code. We use Microsoft 365 and AWS to backup data. We use QuickBooks Online. We use Microsoft Teams to communicate.

Tier 1 Cybersecurity Practices

Cybersecurity requirements are put into practical actions that an SBIR/STTR small business can complete, document, and show as evidence.

1.1 Establish Cybersecurity Responsibilities

DOE requirement: Appoint a Cybersecurity Lead with responsibility and authority to manage the SBC's cybersecurity program.

Implementation

- Document the Cybersecurity Lead's name, role, and backup/contact information.
- Develop and enforce cybersecurity awareness training.
- Maintain a plan that explains how the SBC will meet security requirements to protect systems, research data, intellectual property, and CUI (when applicable). The plan should include the DOE Tier 1 & 2 cybersecurity practices.
- Develop, approve, distribute, and periodically review cybersecurity policies/processes.
- Conduct and document periodic risk assessments; evaluate whether cybersecurity safeguards are implemented and operating effectively.
- Track vulnerabilities, deficiencies, and corrective actions to closure; ensure leadership reviews risks and supports needed resources.
- Update the cybersecurity program after significant organizational, technology, regulatory, or threat changes.

Evidence

SBC's cybersecurity personnel information/ corrective action list and cybersecurity plan (Attachment 1 provided by SBIR/STTR Office, if needed). Submit cybersecurity training awareness program requirements.

1.2 Manage Organizational Assets and Data

DOE requirement: Identify, document, maintain, and regularly update assets that process, store, transmit, or protect business information, intellectual property, and CUI.

Implementation

- Identify, classify, and restrict access to critical intellectual property.
- Maintain an inventory covering relevant data, hardware, software, systems, cloud services, network devices, research/laboratory equipment, and other technology assets.
- Identify authorized and unauthorized assets; remove, disable, or restrict unauthorized devices/services.
- Use the inventory to identify high-value/critical R&D assets and to support risk management, configuration management, incident response, and lifecycle decisions.
- Document important asset details such as owner, purpose, location, version, support status, Internet exposure, and whether sensitive R&D/CUI is handled.
- Review the inventory regularly and whenever assets are added, removed, replaced, or significantly changed.

Evidence

SBC's asset inventory (Attachment 2 provided by SBIR/STTR Office if needed) and process and/or policy for managing assets. SBC's documented data classification process.

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.

Implementation

- Maintain a service-provider list and document the services and access each provider has.
- Assess cybersecurity risk before selection/renewal and after significant incidents or changes.

- Put appropriate security, incident notification, investigation cooperation, and applicable DOE SBIR/STTR requirements in contracts/service agreements.
- Document shared responsibilities for patching, backups, logging, Multi-Factor Authentication (MFA), vulnerability management, incident response, account management, and data protection.
- Limit provider access using least privilege, separate administrative accounts, and MFA for remote access.
- Monitor provider performance/security and review providers at least annually; promptly terminate access when services end.

Evidence

SBC's MSP list found on the inventory list (Attachment 3 provided by SBIR/STTR Office if needed).

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.

Implementation

- Install current security updates before deployment where appropriate.
- Conduct vulnerability scan and patch weaknesses.
- Change defaults on routers, firewalls, access points, switches, servers, network access storage (NAS), printers, voice communication over Internet Protocol (VoIP), laboratory/research equipment, internet of things (IoT)/ operational technology (OT) devices, applications, databases, operating systems, virtual machines (VMs), cloud services, and Software as a Service (SaaS) platforms.
- Disable unnecessary default, guest, and test accounts; if an account cannot be removed, secure it and use MFA) where supported.
- Verify the change before production use and document it in the deployment/configuration process.
- If a device cannot support changing default credentials, document the limitation, apply compensating controls and monitoring, and plan upgrade/replacement.

Evidence

SBC's password policy and/or process that addresses changing default passwords.

1.5 Establish and Enforce Minimum Password Strength

DOE Requirement: Establish and enforce a password policy that makes passwords difficult to guess or crack.

Implementation

- Configure password-protected IT/OT assets for passwords of 16 or more characters when technically feasible, consistent with CISA CPG 2.0.
- Encourage long passphrases and provide an approved password manager where practical.
- Require unique business passwords and prohibit reuse between business and personal accounts.
- Reject common, expected, or compromised passwords where the platform supports this; maintain/update the blocked-password source as appropriate.
- Do not require routine periodic password changes solely because time has passed; change passwords when compromise, exposure, recovery, or another defined event warrants it.
- Where 16 characters are not technically feasible, document the limitation, use compensating controls (such as MFA), log login attempts, and prioritize upgrade/replacement.

Evidence

SBC's password management policy that addresses establishing minimum password strength.

1.6 Implement Multi-Factor Authentication (MFA)

DOE Requirement: Require MFA for access to SBC business/work systems, using the strongest available method.

Implementation

- Require MFA for every employee account used to access SBC systems that handle federal contract and sensitive information, CUI and for all administrator/privileged accounts.
- Enable MFA for email, cloud platforms, virtual private network (VPN)/remote access, collaboration/file sharing, and systems containing federally funded R&D, intellectual property, or CUI.
- Prefer phishing-resistant First Identity Online (FIDO)/web authentication WebAuthn/passkeys or public key infrastructure (PKI)-based methods; if unavailable, prefer app-based methods with number matching over short message service (SMS)/voice.
- Document authenticator issuance, replacement, recovery, and exception procedures.
- Periodically review accounts to confirm MFA remains enabled and unauthorized exceptions are removed.

Evidence

SBC's MFA process and/or policy.

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.

Implementation

- Identify systems, applications, research data, intellectual property, CUI, configurations, installation media, and other recovery information that require backup.
- Back up on a schedule based on business/R&D importance; critical operational systems may require more frequent backup.
- Store at least one protected copy separately from production access; CISA CPG 2.0 recommends offsite/offline storage.
- Protect sensitive backup data, including with cryptographic protection where applicable.
- Test restoration on a recurring basis and no less than annually; validate integrity and check restoration assets for compromise/corruption before use.
- Document test results, correct problems, and review the backup/restoration process at least annually and after significant changes.

Evidence

SBC's backup/restore process and/or policy.

Management Review

The SBC confirms that implementation statements describe current practices unless identified as planned/in progress and that listed evidence can be produced and/or demonstrated if selected for a DOE on-site review. The SBC will update this form as material cybersecurity conditions change.

Cybersecurity Lead / Date	Name: _____ Signature: _____ Date: _____
Principal Investigator / Business Official / Date	Name: _____ Signature: _____ Date: _____

Tier 2: Cybersecurity Practices

Cybersecurity requirements are put into practical actions that an SBIR/STTR small business can complete, document, and show as evidence.

2.1 Separate User and Privileged Administrator Accounts

DOE Requirement: Give administrators a normal account for routine work and a separate privileged account only for administrative tasks.

Implementation

- Use standard accounts for email, web browsing, Microsoft Office/Teams, research, and normal business activity.
- Use privileged accounts only for actions such as account administration, software installation/update, firewall/security configuration, patching, cloud administration, and research/laboratory system administration.
- Protect privileged accounts with MFA, strong unique credentials, and no credential sharing.
- Log privileged functions where supported and periodically review privileged accounts and permissions.
- Immediately remove privileged access when duties change or personnel leave.

Evidence

SBC's access control policy and/or policy that describe separating user and privileged administrator accounts.

2.2 Implement the Principles of Least Privilege

DOE Requirement Give users, administrators, applications, service accounts, and system processes only the access needed to perform authorized duties.

Implementation

- Grant access based on job need and use role-based access where practical.
- Do not grant administrator rights unless required; prevent standard users from privileged actions unless specifically authorized.
- Limit service accounts to required permissions and protect their credentials.
- Review access permissions and role assignments quarterly to align with CISA CPG 2.0; remove unnecessary access promptly.
- Modify or remove access immediately when personnel leave or responsibilities change; log/review privileged activities.

Evidence

SBC's access-control policy and/or process that describes how principles of least privilege are implemented.

2.3 Enable Email Security

DOE Requirement: Protect SBC email from spoofing, phishing, interception, malicious content, and account compromise.

Implementation

- Enable STARTTLS on corporate email infrastructure. (This feature may already be enabled. Please refer to the implementation guide for more information.
- Configure SPF and DKIM and enable DMARC with a policy of reject. (More information can be found on the technical implementation guide).
- Require MFA for company email accounts and enable anti-spam, anti-phishing, anti-malware, malicious-link, and attachment protections available in the platform.
- Protect sensitive information in email using appropriate encryption or approved secure-sharing methods.
- Log/monitor email security events, investigate suspicious activity, train users to recognize/report phishing and business email compromise, and periodically review settings/reports.

Evidence

SBC's email security process and/or policy.

2.4 Utilize Strong Encryption

DOE Requirement: Use strong cryptographic protections for federally funded R&D, intellectual property, credentials, CUI, and other sensitive information at rest and in transit.

Implementation

- Identify sensitive electronic data/file types that require protection.
- Use encryption for laptops, mobile devices, servers, cloud storage, removable media, databases, and backups containing sensitive information as appropriate.
- Use secure protocols such as HTTPS/TLS, SSH, SFTP, and secure VPNs across public/untrusted networks; disable obsolete protocols, weak ciphers, and unsupported algorithms.
- Do not store passwords/credentials in plaintext; use approved secure credential/password management.
- Manage encryption keys securely, limiting access and retiring/rotating keys as appropriate.
- When protecting the confidentiality of CUI, use FIPS-validated cryptography as required by NIST SP 800-171r3 03.13.11; verify cloud-provider encryption and shared responsibilities.

Evidence

SBC's encryption policy and/or process for identifying data at rest and in transit.

2.5 Monitor Unsuccessful Login Attempts

DOE Requirement: Detect, log, limit, and respond to repeated unsuccessful login attempts that may indicate brute force, password spraying, or credential attacks. Detect repeated failed sign-ins and automatically slow, block, lock, or alert on suspicious attempts before an attacker gains access.

Implementation

- Document how unsuccessful login attempts are monitored and managed.
- Capture unsuccessful logins for high-value and important systems, including user/admin accounts, virtual private network (VPN), cloud services, email, and systems protecting organizational information.
- Define a number of consecutive failed attempts and a time period; configure an automatic protective response such as temporary lockout, delay, administrator alert, or another documented measure.
- Alert security/IT personnel on suspicious patterns or deviation from normal behavior and retain the alert/log in a security or ticketing system.
- Regularly review failed-login activity, investigate suspicious authentication behavior, document corrective actions, and periodically review monitoring settings.

Evidence

SBC's login/lockout policy.

2.6 Establish and Maintain an Incident Response Plan

DOE Requirement: Maintain a concise, usable plan for responding to cyber incidents affecting SBC systems, federally funded R&D, intellectual property, sensitive information, and CUI when applicable.

Implementation

- Create a written plan covering likely scenarios such as phishing/account compromise, ransomware/malware, lost/stolen equipment, unauthorized R&D disclosure, cloud compromise, insider activity, and Internet-facing system attacks.
- Assign response roles for leadership, technical investigation, communications, contractual/legal reporting, recovery, and MSP/MSSP coordination.
- Maintain internal and external contact information and define incident severity/escalation criteria.
- Address containment, evidence/log preservation, recovery, communications, and reporting at a high level.
- Exercise the plan with realistic stakeholders at least annually, and update it after exercises, actual incidents, major changes, or identified deficiencies.

Evidence

SBC's approved incident response plan (Attachment 3 provided by SBIR/STTR Office if needed).

2.7 Maintain Incident Response Procedures

DOE Requirement: Maintain repeatable, step-by-step procedures personnel can execute when a suspected or confirmed cyber incident occurs.

Implementation

- Use a simple operational flow: Report → Assess → Contain → Preserve → Eradicate → Recover → Notify/Communicate → Document → Improve.
- Tell employees exactly who to contact and provide a backup communication method if normal systems are unavailable or compromised.
- Define immediate employee actions and authorized technical actions; employees should not conduct their own investigation unless assigned to that role.
- Assess what happened, when, affected accounts/devices/systems/data, whether sensitive R&D/CUI is involved, and severity.
- Document containment, evidence preservation, threat removal, safe recovery, monitoring, incident closure, and lessons learned.
- Define who makes external reporting decisions and how incident communications are coordinated with DOE SBIR/STTR, leadership, providers, partners, and other applicable parties.
- Practice the procedures with a realistic walkthrough/tabletop and update them based on lessons learned.

Evidence

SBC's approved incident response procedure worksheet (Attachment 4 provided by SBIR/STTR Office).

Management Review

The SBC confirms that implementation statements describe current practices, and listed evidence can be produced and/or demonstrated if selected for a DOE on-site audit. The SBC will update this form as cybersecurity conditions change.

Cybersecurity Lead / Date	Name: _____ Signature: _____ Date: _____
Principal Investigator / Business Official / Date	Name: _____ Signature: _____ Date: _____