U.S. DEPARTMENT OF ENERGY | SBIR/STTR

Department of Energy Small Business Innovation Research and Small Business Technology Transfer Tier 2 Supplemental Guide

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

Purpose: Turn Tier 2 cybersecurity requirements into practical actions that a Small Business Innovation Research/Small Business Technology Transfer (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

Table of Contents

How to Use This Guide 6

Tier 2 focuses on implementing four foundational areas: 1.0 Access Controls, 2.0 Data Protection 3.0 Unsuccessful-Login Monitoring, and 4.0 I Incident Response. These are the same core areas identified in the Tier 2 Cybersecurity Implementation Requirements and Evidence Form. The instructions below are reorganized for SBCs that may have a small staff, limited IT support, and extensive use of cloud or managed services. 6

Please Note: A third-party service can provide a security feature, but the 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. 6

What "fully implemented" should mean for an SBC 6

- The technical setting or process is enabled and operating on the systems within scope. 6
- Responsibility is assigned to an employee, owner, IT administrator, MSP, or MSSP. 6
- The SBC has a short-written policy, procedure, or configuration record describing the practice. 6
- Personnel who must follow the practice know what is expected. 6
- If needed, SBC can provide reasonable evidence such as screenshots, exported settings, logs, reports, tickets, policies, or test results. 6
- The SBC reviews and updates (as needed) the practice periodically and after significant system, personnel, or service changes. 6
- Security practices are sufficient at protecting CUI, FCI, and sensitive information from unauthorized disclosure. 6

Important Scope Note 6

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. 6

Tier 2 Quick Planning Estimate 6

Practice 6

Typical hands-on effort 6

Typical calendar time 6

1. Access Controls (Separate User and Privileged Administrator Accounts and Implement the Principles of Least Privilege) 6

8–24 hours 6

1-3 business days 6

2. Secure Email 6

8–24 hours 6

1-3 business days 6

3. Strong Encryption 6

12–40 hours 6

2-5 business days 6

4. Failed Login Monitoring 6

6–24 hours 6

1-3 business days 6

5. Incident Response Plan 6
8–24 hours 6
1-3 business days 6
6. Incident Response Procedures 6
12–40 hours 6
2-5 business days 6
Timing assumption: These estimates are specifically tailored to a DOE SBIR/STTR R&D Small Business Concern (SBC) with 1–25 employees. The estimated 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. 6
Third-Party Services Commonly Seen in Small R&D Environments 7
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. 7
Acronyms 7
Acronym 7
Meaning 7
CISA 7
Cybersecurity and Infrastructure Security Agency 7
CPG 7
Cybersecurity Performance Goal 7
CUI 7
Controlled Unclassified Information 7
DKIM 7
DomainKeys Identified Mail 7
DMARC 7
Domain-based Message Authentication, Reporting, and Conformance 7
FCI 7
Federal Contract Information 7
FIPS 7
Federal Information Processing Standards 7
IAM 7
Identity and Access Management 7
IR 7
Incident Response 7
IRP 7
Incident Response Plan 7
MFA 7

Multi-Factor Authentication 7
MSP 7
Managed Service Provider 7
MSSP 7
Managed Security Service Provider 7
R&D 7
Research and Development 7
SBC 7
Small Business Concern 7
SBIR 7
Small Business Innovation Research 7
SPF 7
Sender Policy Framework 7
STTR 7
Small Business Technology Transfer 7
TLS 7
Transport Layer Security 7
VPN 7
Virtual Private Network 7
1.0 Access Controls 8
Aligned with CS Practice 2.1 Separate User and Privileged Administrator Accounts and 2.2 Implement the Principle of Least Privilege found on the DOE SBIR/STTR Implementation and Evidence Form. 8
2.1 Separate User and Privileged Administrator Accounts 8
2.2 Implement the Principles of Least Privilege 9
2.0 Secure Data 10
Aligned with CS Practice 2.3 Enable Email Security and 2.4 Utilize Strong Encryption found on the DOE SBIR/STTR Implementation and Evidence Form 10
2.3 Enable Email Security 10
Framework Alignment 10
Implementation Steps 10
Can a third-party service provider help? 10
2.4 Utilize Strong Encryption 11
Framework Alignment 11
Implementation Steps 11
Can a third-party service provider help? 12
3.0 Unsuccessful-Login Monitoring 13
Aligned with CS Practice 2.5 Monitor Unsuccessful Login Attempts found on the DOE SBIR/STTR Implementation and Evidence Form. 13
2.5 Monitor Unsuccessful Login Attempts 13
Framework Alignment 13
Implementation Steps 13

Can a third-party service provider help? 13
4.0 Incident Response 14
Aligned with CS Practice 1.7 Maintain System Backups & Restoration Ability found on the DOE SBIR/STTR Implementation and Evidence Form 14
2.6 Establish and Maintain an Incident Response Plan 14
Framework Alignment 15
Implementation Steps 15
Can a third-party service provider help? 15
2.7 Maintain Incident Response Procedures 16
Framework Alignment 16
Implementation Steps 16
Can a third-party service provider help? 17
Primary Sources and Vendor References 18

How to Use This Guide

Tier 2 focuses on implementing four foundational areas: 1.0 Access Controls, 2.0 Data Protection 3.0 Unsuccessful-Login Monitoring, and 4.0 I Incident Response. These are the same core areas identified in the Tier 2 Cybersecurity Implementation Requirements and Evidence Form. The instructions below are reorganized for SBCs 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 the 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 2 Quick Planning Estimate

Practice	Typical hands-on effort	Typical calendar time
1. Access Controls (Separate User and Privileged Administrator Accounts and Implement the Principles of 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

Timing assumption: These estimates are specifically tailored to a DOE SBIR/STTR R&D Small Business Concern (SBC) with 1–25 employees. The estimated 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	Meaning
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goal
CUI	Controlled Unclassified Information
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
IAM	Identity and Access Management
IR	Incident Response
IRP	Incident Response Plan
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
R&D	Research and Development
SBC	Small Business Concern
SBIR	Small Business Innovation Research
SPF	Sender Policy Framework
STTR	Small Business Technology Transfer
TLS	Transport Layer Security
VPN	Virtual Private Network

1.0 Access Controls

Aligned with CS Practice 2.1 Separate User and Privileged Administrator Accounts and 2.2 Implement the Principle of Least Privilege found on the DOE SBIR/STTR Implementation and Evidence Form.

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.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.01.05 Least Privilege; 03.01.06 Privileged Accounts; 03.01.07 Privileged Functions	Maintain separate standard and privileged accounts, require MFA and unique credentials for privileged access, and prevent normal users from performing privileged functions.
CISA CPGs v2.0	3.G Administrators Maintain Separate User and Privileged Accounts	Use separate administrative access, rather than day-to-day accounts, for privileged actions.

Implementation Steps

1. Identify the SBC's high-value systems and accounts: company email, cloud storage, repositories, source-code platforms, research servers, laboratory systems, finance/HR systems, and cloud administration portals.
2. List who currently has administrator, owner, root, super-admin, global-admin, or equivalent privileges.
3. Create or retain a standard user account for each administrator's routine work. Use a separate privileged account only for administrative actions.
4. Enable MFA on every privileged account and do not share administrator credentials.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Common Service / Provider	Can it help?	SBC action in the service	Vendor source
Microsoft 365 / Microsoft Entra	Yes	Assign only required Microsoft Entra roles; use separate administrator accounts; require MFA for administrators; review role assignments.	Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices
Google Workspace	Yes	Use administrator roles with only required privileges; avoid using a super-admin account for daily work; enforce	Google Workspace Admin Help: https://support.google.com/a/answer/2405986

		2-Step Verification for administrators.	
AWS	Yes	Use IAM roles and policies that grant least privilege; protect privileged identities with MFA; avoid routine use of the root user.	AWS IAM User Guide: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Evidence Required: SBC's access control policy and/or policy that describe separating user and privileged administrator accounts.	Approximate implementation time: 1-3 business days

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.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.01.05 Least Privilege; 03.01.06 Privileged Accounts; 03.01.07 Privileged Functions	Grant access based on job need, remove unnecessary privileges, and periodically review access.
CISA CPGs v2.0	3.H Implement the Principles of Least Privilege	Grant only the access needed for the job and remove access that is no longer needed.

Implementation Steps

1. Remove administrator rights from personnel who do not need them. Prevent standard users from installing software or changing security settings unless specifically approved.
2. Use groups or roles where practical so permissions follow job functions rather than being assigned one file or user at a time.
3. Review privileged and user access at least annually and whenever someone leaves, changes duties, or no longer needs access.
4. Document who approved privileged access, what systems it covers, and when it was last reviewed.

Can a third-party service provider help?

Yes -- the same identity and access-management platforms used for Section 2.1 (Microsoft Entra, Google Workspace, AWS IAM) also support role-based, least-privilege access. See Section 2.1 for vendor-specific enablement options.

Evidence Required: SBC's access-control policy and/or process that describes how principles of least privilege are implemented.	Approximate implementation time: 1-3 business days

2.0 Secure Data

Aligned with CS Practice 2.3 Enable Email Security and 2.4 Utilize Strong Encryption found on the DOE SBIR/STTR Implementation and Evidence Form

2.3 Enable Email Security

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

Reduce phishing, spoofing, malware, account takeover, and accidental disclosure by using the security features already available in SBC's email service.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.05 Identification and Authentication; 03.13.08 Transmission Confidentiality and Integrity; 03.14 System and Information Integrity	Protect email identities, transmissions, and users from malicious content and unauthorized access.
CISA CPGs v2.0	Email Security (2.M) and phishing-resistant/MFA-related identity protections	Authenticate company email, reduce spoofing, enable filtering, and protect email accounts.

Implementation Steps

1. Require MFA for all company email accounts, with stronger/phishing-resistant methods where supported.
2. Confirm anti-spam, anti-phishing, and anti-malware protections are enabled in the email platform.
3. Configure the company domain with SPF and DKIM, then enable DMARC. Start with monitoring if needed, review reports, and move toward an enforcement policy after legitimate senders are identified.
4. Confirm TLS is used for normal mail transport. For CUI or particularly sensitive R&D information, use an approved secure method that provides the required confidentiality rather than assuming ordinary email is sufficient.
5. Configure suspicious messages, attachments, and links to be blocked, quarantined, or otherwise handled by the email security service.
6. Enable security/audit logging and review suspicious sign-ins, forwarding rules, mailbox changes, and reported phishing.
7. Train personnel to report phishing, spoofing, business email compromise, unexpected MFA prompts, and suspicious requests for R&D or financial information.
8. Review email-security settings after domain, provider, or major configuration changes and at least annually.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Service / Provider	Can it help?	SBC action in the service	Vendor source
Microsoft 365 / Exchange Online	Yes	Use Microsoft 365 MFA/Conditional Access as licensed; configure SPF, DKIM and DMARC; use Exchange Online Protection and	Microsoft Learn: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about and https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dmarc-configure

		Microsoft Defender features available to the tenant; review audit/sign-in data.	
Google Workspace / Gmail	Yes	Enforce 2-Step Verification; configure SPF, DKIM and DMARC for the domain; use Gmail spam/phishing protections; use Email Log Search and security investigation features available to the edition.	Google Workspace Admin Help: https://support.google.com/a/answer/1068509 ; https://support.google.com/a/answer/174124 ; https://support.google.com/a/answer/2466563
Third-party email security / MSP	Often	An MSP or email-security provider can configure DNS records, filtering and alerting. The SBC should retain administrative visibility and confirm who receives alerts and who can change mail settings.	Use the provider's current administration and security documentation for the specific service purchased.

Important: SPF, DKIM, and DMARC protect the SBC's domain from spoofing and improve message authentication, but they do not replace MFA, malware filtering, user training, or appropriate encryption for sensitive data.

Evidence Required: SBC's email security process and/or policy.	Approximate implementation time: About 2–4 hours when the domain and email service are already established; up to 1–3 business days when SPF, DKIM, DMARC, DNS changes, mail-flow testing, or licensing changes are required.

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.

Protect sensitive R&D information, credentials, backups, and CUI from disclosure if a device, account, storage location, or network connection is compromised.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.13.08 Transmission Confidentiality and Integrity; 03.13.11 Cryptographic Protection; 03.08.09 System Backup	Protect CUI in transit and at rest using required cryptographic protections; protect backup information.
CISA CPGs v2.0	Strong and Agile Encryption (2.K)	Use strong encryption, manage cryptographic technology, and replace weak or obsolete methods.

Implementation Steps

1. Identify where federally funded R&D, intellectual property, credentials, and CUI are stored and transmitted.
2. Enable full-disk or device encryption on laptops and other portable systems that store sensitive information.

3. Confirm cloud storage, servers, databases, backups, and removable media containing sensitive information are encrypted at rest.
4. Use secure protocols such as HTTPS/TLS, SSH, SFTP, or an approved VPN when sensitive information crosses public or untrusted networks.
5. For CUI, verify that cryptography used to protect confidentiality is FIPS-validated as required by NIST SP 800-171 Rev. 3 and the applicable system/service architecture.
6. Disable obsolete protocols and weak cryptographic options when the SBC controls those settings.
7. Limit access to encryption keys and secrets. Use the cloud provider's key-management capability where appropriate and document who can administer keys.
8. Review encryption settings after major system/service changes and periodically for continued suitability.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Service / Provider	Can it help?	SBC action in the service	Vendor source
Microsoft Windows / Microsoft 365 / Azure	Yes	Use BitLocker/device encryption where supported; use Microsoft 365 and Azure encryption capabilities; use Key Vault for managed keys when appropriate; verify the specific service/configuration used for CUI.	Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ and https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
Google Workspace / Google Cloud	Yes	Use provider encryption features and secure transport; for Google Cloud, use Cloud KMS/CMEK where appropriate. For CUI, verify the service and cryptographic implementation meet contractual requirements.	Google Cloud: https://cloud.google.com/docs/security/encryption/default-encryption and https://cloud.google.com/kms/docs
AWS	Yes	Use encryption at rest for services such as S3/EBS/RDS as applicable; use TLS for data in transit; manage keys with AWS KMS where appropriate; validate the architecture for CUI.	AWS: https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/data-encryption.html and https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

Important: Do not treat a provider statement that 'data is encrypted' as the only evidence for CUI. The SBC should verify the specific service, configuration, cryptographic boundary, and contractual requirements that apply to its environment.	
Evidence Required: SBC's encryption policy/process identifying data at rest and in transit.	Approximate implementation time: About 2–6 hours when built-in device and cloud encryption is available; 1–3 business days when the SBC must encrypt servers, removable media, databases, backups, or validate FIPS status across several services.

3.0 Unsuccessful-Login Monitoring, and 4.0 I Incident Response

3.0 Unsuccessful-Login Monitoring

Aligned with CS Practice 2.5 Monitor Unsuccessful Login Attempts found on the DOE SBIR/STTR Implementation and Evidence Form.

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.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.01.08 Unsuccessful Logon Attempts; 03.03 Audit and Accountability	Limit consecutive invalid logon attempts, take an automated protective action, generate audit records, and review relevant activity.
CISA CPGs v2.0	Account protection, logging, and monitoring goals	Use platform controls and logs to identify brute-force, password-spraying, and suspicious authentication activity.

Implementation Steps

1. Identify systems where failed sign-ins matter: email, cloud identity, VPN, remote access, R&D repositories, research servers, finance/HR, and administrator portals.
2. Configure each system to limit repeated unsuccessful logon attempts within a defined period and to take an automated action such as temporary lockout, delay/throttling, or another documented protective measure.
3. Enable authentication and security logging for user and administrator sign-ins.
4. Enable alerts or routine review for repeated failures, impossible/unusual sign-ins, password spraying, or repeated attempts against privileged accounts.
5. Assign a person or provider to review authentication alerts/logs and define what requires investigation.
6. When suspicious activity is found, preserve relevant logs, reset or disable affected credentials as appropriate, revoke sessions where supported, and document the response.
7. Periodically test or review the configuration to confirm failed-login protections and logging still work.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Service / Provider	Can it help?	SBC action in the service	Vendor source

Microsoft Entra ID / Microsoft 365	Yes	Use smart lockout and identity protection/sign-in logs available to the tenant; configure alerting and review risky or repeated sign-in activity.	Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout and https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins
Google Workspace	Yes	Use login audit/security investigation features available to the edition; review failed or suspicious login events and configure alerting rules where supported.	Google Workspace Admin Help: https://support.google.com/a/answer/4580120
AWS	Yes	Use CloudTrail and IAM/security services to record and investigate authentication and API activity; configure alarms/detections appropriate to the environment.	AWS CloudTrail: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

Important: Exact lockout thresholds should be chosen for SBC's environment. NIST SP 800-171 Rev. 3 requires the organization to define the number of consecutive invalid attempts and the automated response; it does not prescribe one universal number for every SBC.

Evidence Required: SBC's login/lockout policy.	Approximate implementation time: About 1–3 hours for one cloud identity platform; 4–8 hours when the SBC must configure several systems, VPNs, servers, research applications, or centralized logging.

4.0 Incident Response

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

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, federal contract and sensitive information, and CUI when applicable.

Create a short, usable plan that tells the SBC who is responsible, what events count as incidents, who must be contacted, and how the business will contain, recover from, and learn from an incident.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.06.01 Incident Handling; 03.06.02 Incident Monitoring, Reporting, and Response Assistance; 03.06.03 Incident Response Testing	Establish incident handling capability, track/report incidents, obtain response support, and test incident response.
CISA CPGs v2.0	Incident Response Plans (2.S) and incident reporting/readiness goals	Maintain an actionable plan with roles, contacts, escalation, communications, and recovery.

Implementation Steps

1. Name the incident response lead and backups. For a very small SBC, this may be the owner, cybersecurity lead, IT administrator, or designated MSP/MSSP contact.
2. List likely incident types: phishing/account compromise, ransomware, malware, lost/stolen equipment, unauthorized disclosure of R&D/CUI, compromised cloud accounts, insider activity, and attacks on internet-facing systems.
3. Define roles for technical investigation, management decisions, communications, legal/contractual reporting, evidence preservation, and recovery.
4. Maintain an incident contact list that includes internal contacts and, as applicable, the MSP/MSSP, cyber insurer, legal counsel, cloud providers, and DOE SBIR/STTR reporting contact.
5. Define severity and escalation criteria so personnel know when a security event becomes an incident requiring management involvement or external reporting.
6. Describe at a high level how affected accounts/devices will be isolated, logs/evidence preserved, threats removed, and systems/data restored.
7. Conduct a tabletop exercise using a realistic R&D scenario and document what worked and what must be improved.
8. Update the plan after incidents, significant system/personnel changes, and exercises.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Service / Provider	Can it help?	SBC action in the service	Vendor source
Microsoft 365 / Azure	Yes	Microsoft security portals can provide alerts, logs, device/account actions, and investigation information used during response. The SBC must still maintain its own roles, reporting requirements, and response plan.	Microsoft incident response guidance: https://learn.microsoft.com/en-us/security/operations/incident-response-playbook
Google Workspace / Google Cloud	Yes	Security investigation, audit, account suspension/session controls, and cloud logging can support investigation and containment depending on edition/service.	Google Workspace security center: https://support.google.com/a/answer/7492006 ; Google Cloud incident response: https://cloud.google.com/security/incident-response

MSP / MSSP / cyber insurer	Yes	A provider can supply 24/7 monitoring, technical investigation, containment support, and incident-response expertise if included in the contract. The SBC should document exactly what the provider will do and how to contact it during an incident.	Use the provider's current incident-response service description, contract/SLA, and escalation instructions.

Important: The plan can be concise. For a small SBC, a practical 3–8 page plan with current contacts, roles, reporting triggers, and recovery actions is often more useful than a long document that personnel cannot use during an incident.

Evidence Required: SBC's Incident Response Plan (attachment 3).	Approximate implementation time: About 3–6 hours for a small SBC with a simple environment; 1–2 business days if multiple facilities, cloud providers, laboratories, legal/reporting obligations, or an MSP/MSSP must be coordinated.

2.7 Maintain Incident Response Procedures

DOE Requirement: Turn the incident response plan into repeatable, step-by-step actions personnel can follow during an actual cybersecurity incident.

Framework Alignment

Framework	Practice / Requirement	How this guide applies it
NIST SP 800-171 Rev. 3	03.06.01 Incident Handling; 03.06.02 Incident Monitoring, Reporting, and Response Assistance; 03.06.03 Incident Response Testing	Use repeatable actions to detect, analyze, contain, eradicate, recover, report, and test incident response.
CISA CPGs v2.0	Incident-response readiness and reporting goals	Document operational actions, escalation, communications, and recovery so personnel know what to do.

Implementation Steps

1. Write one simple employee reporting procedure: what to report, who to contact, and a backup contact method if normal email or systems are unavailable.
2. Define immediate employee actions, such as stop interacting with a suspicious message, preserve the message, report it, and avoid deleting evidence or conducting an unauthorized investigation.
3. Define technical triage steps: determine what happened, when it happened, what accounts/devices/data are affected, whether R&D or CUI is involved, and how serious the incident is.
4. Document authorized containment actions such as isolating a device, disabling an account, revoking sessions, blocking malicious traffic, or temporarily restricting access.
5. Document how logs, messages, files, timestamps, screenshots, and other relevant evidence will be preserved.
6. Document eradication and recovery steps, including removal of malicious persistence, credential reset, restoration from known-good backups, validation, and enhanced monitoring before normal operations resume.
7. Document notification and escalation requirements. Include the DOE SBIR/STTR Office contact specified by the program and any other contractual or legal reporting obligations applicable to the award.

8. Maintain an incident record/register showing what occurred, actions taken, reporting, recovery, and lessons learned.
9. Practice the procedures through a walkthrough/tabletop and revise them when gaps are identified.

Can a third-party service provider help?

Yes. For many small R&D businesses, cloud identity, email, endpoint, logging, and security services can provide the technical features needed. The SBC remains responsible for selecting the settings, assigning responsible personnel, reviewing alerts/reports, and documenting that the practice is operating as intended.

Service / Provider	Can it help?	SBC action in the service	Vendor source
Microsoft security tools	Yes	Use tenant sign-in/audit logs, Defender/security alerts where licensed, account disable/reset/session revocation, endpoint isolation where available, and evidence exports to support the SBC procedure.	Microsoft security operations documentation: https://learn.microsoft.com/en-us/security/operations/
Google Workspace / Google Cloud	Yes	Use audit/security investigation tools, account suspension/session reset, Gmail investigation tools, and cloud logging/response capabilities available to the service.	Google Workspace security investigation: https://support.google.com/a/answer/7575955 ; Google Cloud security: https://cloud.google.com/security
MSP / MSSP	Yes	The provider may perform triage, containment, log collection, eradication, and recovery. The SBC procedure should state what employees do first, how the provider is contacted, what authority the provider has, and what the SBC retains responsibility for.	Use the provider's current contract, runbooks, emergency contact instructions, and service documentation.

Important: The DOE SBIR/STTR Office email address for incident-reporting is csduediligence@doe.gov. The SBC should also follow any reporting timeframes and channels stated in its award, contract, or current DOE instructions.

Evidence Required: SBC's approved incident response procedure worksheet (attachment 4).	Approximate implementation time: About 4–8 hours for core procedures; 1–3 business days if the SBC develops separate procedures/playbooks for phishing, ransomware, lost devices, cloud-account compromise, and CUI exposure.

Primary Sources and Vendor References

- NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: https://csrc.nist.gov/pubs/sp/800/171/r3/final
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs), Version 2.0 and current CPG resources: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
- NIST FIPS 140-3, Security Requirements for Cryptographic Modules: https://csrc.nist.gov/pubs/fips/140-3/final
- Microsoft Learn security and administration documentation: https://learn.microsoft.com/
- Google Workspace Admin Help: https://support.google.com/a/
- Google Cloud security documentation: https://cloud.google.com/security
- AWS security, IAM, CloudTrail, encryption, and KMS documentation: https://docs.aws.amazon.com/

Vendor interfaces, product names, licensing, and feature availability can change. SBCs should verify vendor-specific configuration steps against the vendor's current documentation at the time of implementation.