Cyber Risk Management FAQs

Protecting Innovation from Research to Commercialization

DOE SBIR/STTR Security Risk Management • Updated October 2026

INDEX OF FAQs by Section

Questions based on Topics	Relevant FAQs
Homepage: Federal mandate and applicant expectations	1–7
Homepage: Self-assessment and submission	8–17
Tier 1: Cybersecurity leadership (1.1)	4, 5, 18
Tier 1: Assets and MSPs (1.2–1.3)	19–21
Tier 1: Passwords and MFA (1.4–1.6)	22–24
Tier 1: Backup and recovery (1.7)	25
Tier 2: Access controls (2.1–2.2)	26–27
Tier 2: Email and encryption (2.3–2.4)	28–29
Tier 2: Unsuccessful-login monitoring (2.5)	30
Tier 2: Incident response (2.6–2.7)	31–32
Homepage: Risk ratings and audit procedures	33–35

Section 1: General Questions About DOE Cybersecurity Requirements

1. Why does DOE require small businesses to complete cybersecurity due diligence?

- DOE requires cybersecurity due diligence to help protect federally funded research, intellectual property, sensitive business information, and technologies developed through SBIR/STTR awards.
- The process helps DOE identify potential cybersecurity risks and encourages businesses to establish safeguards that protect their research and support commercialization.

2. Does every SBIR/STTR applicant need to complete a cybersecurity self-assessment?

- Requirements depend on the phase, funding opportunity, and release. Phase II applicants should follow the cybersecurity instructions published for their specific DOE funding opportunity.
- Some releases have different reporting requirements. For example, FY 2025 Phase II Release 2 Applied Science requires reporting of cybersecurity practices with supporting evidence instead of using the standard self-assessment process.

3. Does DOE expect a small business to have the same cybersecurity capabilities as a large company?

- DOE's approach is designed to be practical, risk-based, and scalable. A small business may be able to meet many requirements using existing commercial security tools, cloud services, and documented processes.
- The important thing is demonstrating that the required safeguards are appropriately implemented and operating in the company's environment.

4. Do we need to hire a full-time cybersecurity employee?

- The Tier 1 requirement is to appoint a Cybersecurity Lead with responsibility and authority to manage the company's cybersecurity program.
- The position does not necessarily have to be a dedicated, full-time cybersecurity role. Depending on the company's size and capabilities, an owner or qualified employee may perform this function, with support from external IT professionals.

5. Can our IT contractor or Managed Service Provider handle cybersecurity for us?

- Yes. A Managed Service Provider (MSP) or Managed Security Service Provider (MSSP) can help implement and maintain cybersecurity safeguards.
- However, your business remains responsible for making sure the safeguards are configured correctly, maintained, monitored, and documented. Outsourcing IT support does not transfer the company's accountability.

6. What is the difference between Tier 1 and Tier 2 cybersecurity requirements?

- Tier 1 focuses on foundational cybersecurity practices, including assigning cybersecurity responsibilities, identifying assets and service providers, securing passwords and accounts, implementing MFA, and maintaining backups.
- Tier 2 addresses additional protections, including privileged account separation, least privilege, email security, encryption, unsuccessful-login monitoring, and incident response planning and procedures.
- Applicants should follow their release-specific instructions to determine when each tier must be completed.

7. Does DOE require our company to obtain CMMC certification or NIST SP 800-171 certification?

- The DOE cybersecurity self-assessment does not automatically require every applicant to obtain CMMC certification or a separate NIST certification.
- NIST SP 800-171 and CMMC requirements depend on applicable contracts, the type of information handled, and other governing requirements. Businesses handling CUI should determine the specific requirements applicable to their systems and awards.

Section 2: Completing the Cybersecurity Self-Assessment

8. Where can I find the cybersecurity self-assessment forms?

- Use the cybersecurity instructions and resources associated with your current DOE SBIR/STTR funding opportunity.
- The Tier 1 and Tier 2 Self-Assessment Forms identify the cybersecurity practices being evaluated and the evidence associated with each requirement.
- Make sure you use the forms and instructions applicable to your phase and release.

9. How do I complete the self-assessment?

- Review each requirement and select the status that accurately describes your current cybersecurity practices:
    - Fully Implemented
    - Partially Implemented
    - Not Implemented
    - Unknown
- Identify available supporting evidence and complete the required company information.
- Do not describe a planned safeguard as already implemented.

10. What is the difference between Fully Implemented and Partially Implemented?

- Fully Implemented means the required practice is operating across the applicable systems, accounts, and processes.
- Partially Implemented means some parts of the requirement are in place, but the complete requirement has not yet been satisfied.
- For example, if MFA is enabled for company email but not other applicable business systems, the MFA requirement may be only partially implemented.

11. What should I select if I do not understand a requirement?

- Select Unknown if you cannot determine whether a safeguard is implemented.
- Consult your Cybersecurity Lead, IT administrator, or service provider to determine the actual status.
- It is better to identify uncertainty than to report a safeguard as implemented without supporting evidence.

12. Can I select Fully Implemented if we are planning to purchase or configure a security product?

- No. A planned action does not count as an implemented safeguard.
- Select the status that reflects the company's current practices. Once the product or process is implemented, configured, and operating, update the supporting information accordingly.

13. What kind of evidence does DOE expect?

- Evidence depends on the requirement and may include:
  - Cybersecurity policies and procedures
  - Asset inventories
  - Managed service provider lists
  - Password and MFA policies
  - Security configuration records
  - Backup and restoration procedures
  - Access control documentation
  - Email security and encryption policies
  - Incident response plans and procedures
- Provide the evidence identified in the applicable self-assessment and submission instructions.

14. Do we need to purchase expensive cybersecurity software to satisfy the requirements?

- Not necessarily. Many capabilities may already be available through your company's existing email service, operating systems, cloud platforms, or managed IT services.
- For example, commercial platforms may offer MFA, access controls, security logging, email protections, and backups.
- However, having a feature included in a subscription does not mean it is implemented. The feature must be configured and used appropriately.

15. Who is responsible for signing or approving the self-assessment?

- An owner, executive, or authorized business representative should review the self-assessment and confirm that the information is complete and accurate.
- The Cybersecurity Lead may prepare technical responses and collect evidence, but management is responsible for reviewing the company's submission.

16. Can we update our cybersecurity self-assessment after making improvements?

Your company should maintain accurate, current cybersecurity documentation and update its records after making significant changes.
If an assessment has already been submitted, follow DOE's instructions to determine whether and how revised responses or additional evidence may be provided.

17. When must the cybersecurity self-assessment be submitted?

- The deadline is determined by the applicable funding opportunity, phase, release, and amendments.
- Applicants should consult their specific DOE instructions rather than assume that every SBIR/STTR cybersecurity assessment has the same deadline.

Section 3: Tier 1 Cybersecurity Requirements

18. What does DOE expect from our Cybersecurity Lead?

- The Cybersecurity Lead is responsible for coordinating the company's cybersecurity activities, maintaining relevant documentation, identifying gaps, and supporting implementation of required safeguards.
- The company should clearly identify who holds this responsibility and provide the cybersecurity personnel information and other evidence requested under Tier 1 Practice 1.1.

19. What assets must be included in our inventory?

- Your inventory should identify relevant technology that processes, stores, transmits, or protects business information, intellectual property, research information, or CUI.
- Examples include employee laptops, servers, laboratory equipment, cloud storage, research platforms, network devices, and applicable software or services.
- The inventory should be maintained and updated as the environment changes.

20. Do we need to include employees' personal computers in the assessment?

- Yes, if personally owned computers are used to access or process information supporting the company's research or business activities, they should be considered when describing the environment and identifying applicable cybersecurity safeguards.
- The Tier 1 form explicitly includes company-owned and personally owned computers used for research and development.

21. Do Microsoft 365, Google Workspace, AWS, and other cloud services need to be included?

- Yes, when these services support your business operations, research, data storage, collaboration, or cybersecurity.
- The business environment description should identify relevant cloud services and outside providers, especially when they store, process, monitor, or have access to sensitive company information.

22. How do we demonstrate that default passwords have been changed?

- Your company should maintain a policy or procedure explaining how manufacturer or vendor default accounts and passwords are changed or disabled before systems are placed into use.
- Examples may include device configuration checklists, deployment procedures, or other records that demonstrate the practice is followed.
- Do not include actual passwords in the evidence submitted to DOE.

23. What does DOE expect in a password policy?

- The policy should describe how your company establishes and enforces passwords that are difficult to guess or crack.
- It should apply to the relevant systems and accounts and explain the company's password management practices.
- Your submission should identify the policy or process supporting Tier 1 Practice 1.5.

24. Is MFA required if we already use strong passwords?

- Tier 1 Practice 1.6 requires MFA for access to the company's business and work systems, using the strongest available method.
- Strong passwords are important, but they do not replace MFA.
- The company should assess which systems support MFA, whether it is enabled, and whether the practice meets the applicable requirement.

25. Is using cloud storage enough to satisfy the backup requirement?

- Not automatically.
- Tier 1 Practice 1.7 requires the company to maintain the information and configurations needed to restore research and development operations after events such as ransomware, hardware failure, or accidental loss.
- Cloud storage or synchronization alone may not provide the ability to recover deleted, corrupted, or encrypted information.
- The company should have a documented backup and restoration process and verify that recovery is possible.

Section 4: Tier 2 Cybersecurity Requirements

26. Why do administrators need separate accounts?

- Tier 2 Practice 2.1 requires administrators to use a normal account for routine work and a separate privileged account for administrative activities.
- This helps reduce the risk of an attacker gaining administrative privileges if a regular account is compromised.
- For example, an IT administrator should use a standard account for email and everyday business activities and a separate administrative account for changing security settings.

27. What does least privilege mean for a small business?

- Least privilege means providing employees, contractors, applications, and system accounts only the access necessary to perform their authorized responsibilities.
- For example, an employee working on financial reports may not need administrative access to research servers, source-code repositories, or security configurations.
- Access should reflect job responsibilities rather than giving every employee unrestricted permissions.

28. What email security measures does DOE expect?

- Tier 2 Practice 2.3 addresses protecting company email from spoofing, phishing, interception, malicious content, and account compromise.
- Businesses should review their email security settings and maintain an email security policy or process.
- A commercial email provider may supply useful security capabilities, but the company must determine whether the necessary protections are enabled and configured.

29. What does strong encryption mean, and when should we use it?

- Encryption helps protect information from unauthorized access or disclosure.
- Tier 2 Practice 2.4 addresses protection of federally funded research, intellectual property, credentials, CUI, and other sensitive information both at rest and in transit.
- Data at rest includes information stored on computers, servers, and cloud platforms. Data in transit includes information being transmitted through networks, email, or file-sharing services.
- The company should document the encryption protections used and confirm that they meet applicable information-handling requirements.

30. Why does DOE require monitoring of unsuccessful login attempts?

- Repeated failed login attempts may indicate that someone is attempting to guess passwords or gain unauthorized access.
- Tier 2 Practice 2.5 requires businesses to detect, log, limit, and respond to suspicious unsuccessful login attempts.
- Security measures may include account lockout, login throttling, alerts, or automated restrictions, depending on the system.

31. What is the difference between an Incident Response Plan and Incident Response Procedures?

- An Incident Response Plan describes how the company organizes and manages its response to cybersecurity incidents. It identifies responsibilities, communication, and overall response arrangements.
- Incident Response Procedures provide specific instructions employees can follow when an incident occurs.
- For example, the plan may identify who leads the response, while a procedure explains what to do when an employee suspects a ransomware infection.
- Tier 2 Practices 2.6 and 2.7 address these separately.

32. Does a very small company still need an Incident Response Plan?

- The Tier 2 requirements apply according to the applicable DOE funding opportunity and release.

- A small business does not necessarily need a lengthy incident response document. A concise, practical plan can identify who responds, how incidents are reported, how affected systems are handled, and how the business recovers.
- The plan and procedures should be realistic for the company's size, systems, and personnel.

Section 5: Risk Ratings, Audits, and Corrective Actions

33. What happens if DOE determines that our company has cybersecurity weaknesses?

- According to the DOE cybersecurity due diligence guidance, businesses may receive a Low, Medium, or High cybersecurity risk rating.
- The homepage describes an opportunity for businesses with Medium or High ratings to improve their cybersecurity posture before the project start date and reduce their risk to an acceptable level.
- Businesses should follow DOE's specific communication and instructions regarding any identified gaps.

34. Will DOE conduct an audit of our company's cybersecurity practices?

- The DOE homepage indicates that the SBIR/STTR Office may conduct on-site audits to validate information reported in the Implementation & Evidence Form.
- DOE may arrange a discovery meeting to discuss the required evidence and audit process.
- The purpose is to verify that reported cybersecurity safeguards are implemented and operating as described.

35. What should we do to prepare for a cybersecurity audit?

- Review your self-assessment responses and ensure that the supporting evidence is available, accurate, and current.
- Identify the people responsible for each cybersecurity practice and be prepared to explain how those practices work.
- For example, your company should be able to explain how MFA is enforced, how assets are inventoried, how backups are maintained, and how cybersecurity incidents would be handled.
- You should also be prepared to demonstrate applicable safeguards rather than relying solely on written policy statements.