Cybersecurity Due Diligence

Protecting Innovation from Research to Commercialization

DOE SBIR/STTR Security Risk Management • Updated October 2026

WHY THIS MATTERS Small Business Innovation Research (SBIR)/ Small Business Technology Transfer (STTR) cybersecurity due diligence is more than a compliance checkpoint. It helps protect federally funded R&D, intellectual property, sensitive information, and the small business's ability to transition technology into the U.S. marketplace.

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.

A Current Federal Mandate

Congress requires federal agencies that operate SBIR or STTR programs to establish and implement due diligence programs to assess security risks presented by small businesses seeking federally funded awards. **15 U.S.C. § 638(vv)** directs agencies to use a risk-based approach that includes cybersecurity practices, patent analysis, employee analysis, foreign ownership, financial ties and obligations, and required foreign-relationship disclosures.

The **Small Business Innovation and Economic Security Act of 2026 (Public Law 119-83; S. 3971)**, signed April 13, 2026, reauthorized the SBIR/STTR programs and strengthened the research-security framework. The current authorization extends the statutory due diligence program through **September 30, 2031**.

What Changed in 2026

The 2026 law expands the security picture beyond traditional cyber controls. DOE's current Security Risk Management guidance explains that reviews now also consider:

- Foreign affiliations of covered individuals, owners, and other key personnel with entities in a foreign country of concern (FCOC).
- Investment relationships with individuals or entities in an FCOC.
- Technology licensing agreements or joint ventures involving individuals or entities in an FCOC.
- Business relationships between key personnel and individuals or entities in an FCOC.
- Relationships with individuals or entities appearing on specified Federal sanctions and restricted-party lists.

For SBIR/STTR purposes, DOE identifies the current foreign countries of concern as **the People's Republic of China, the Democratic People's Republic of Korea, the Russian Federation, and the Islamic Republic of Iran**, plus any other country later designated by the Secretary of State.

How DOE Applies Cybersecurity Due Diligence

DOE evaluates security risk separately from the scientific and technical merit review. Phase II small business applicants are assessed for cybersecurity business-practice risk, and Phase II applicants are required to submit a cybersecurity self-assessment as specified in the applicable funding opportunity. In addition, Phase I awardees are encouraged to strengthen their cybersecurity posture before applying for Phase II.

> **For Only - FY 2025 Phase II Release 2 Applied Science**: The self-assessment will not be used, instead reporting of requirements along with body of evidence submission will be required. Please see SBIR/STTR Cybersecurity Self-Assessment section for more details.

1 ASSESS	2 REDUCE RISK	3 PROTECT TRANSITION
Review cybersecurity practices and the small business operating environment using DOE's risk-based process.	Implement practical safeguards that reduce exposure of R&D, sensitive information, systems, and intellectual property.	Maintain a stronger security foundation as the technology moves toward Phase II execution and commercialization.

Cybersecurity Baseline: Practical, Risk-Based, and Scalable

DOE's cybersecurity requirements are derived from the Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs), National Institute of Standards and Technology_ Special Publications 800-171 Revision 3 (NIST SP 800-171r3) and aligned with the NIST Cybersecurity Framework. The objective is to reduce the likelihood that federally funded R&D or sensitive information is compromised or disclosed without authorization, including to foreign countries of concern.

DOE's SBIR/STTR Cybersecurity Due Diligence efforts help protect Small Business Concerns (SBCs) against unauthorized access to or disclosure of sensitive information, including federally funded research, intellectual property, and proprietary technologies. In addition to assessing cybersecurity risks, DOE supports SBCs in establishing or improving cybersecurity practices appropriate to their research activities, operating environments, and level of risk. Through practical implementation guidance, learning resources, and opportunities to address identified gaps, these efforts help small businesses strengthen safeguards for sensitive information throughout research, development, and commercialization.

For small businesses, this means focusing on high-value protections that can scale with the company: clear cybersecurity responsibilities, asset and account management, multifactor authentication, least privilege, secure configurations, encryption, email protections, backups and restoration, vulnerability management, incident response, and workforce awareness. Many foundational capabilities can be enabled through commercial-grade cloud and IT services already used by small businesses.

IMPORTANT DISTINCTION NIST SP 800-171 Rev. 3 and CMMC are useful reference points listed in DOE's resource set, but they should not be described as automatically applicable to every DOE SBIR/STTR applicant. Applicability depends on the award, contract terms, information handled (for example, CUI), and other governing requirements.

What Applicants Should Expect

Understand the scope. Identify the people, systems, cloud services, devices, research data, intellectual property, and sensitive information supporting the SBIR/STTR effort.

Complete the required assessment. Phase II applicants should follow the current DOE funding opportunity and cybersecurity self-assessment instructions.

Address identified gaps. Use the assessment to prioritize safeguards and document implementation evidence.

Treat security as part of commercialization. A defensible cybersecurity posture helps protect the technology, business relationships, and data needed to move from federally funded R&D to market adoption.

DOE Applicant Resources

- **SBIR/STTR Cybersecurity Self-Assessment:** Use the current DOE instructions and funding opportunity requirements.
- **Risk Rating Information:** Understand how cybersecurity risk is evaluated and what may require mitigation.
- **Learning and Education Resources:** Use practical training and implementation guidance to improve cybersecurity maturity.
- **Auditing Information:** Prepare supporting evidence that demonstrates safeguards are implemented and operating.
- **Cyber Risk Management FAQs:** Clarify common questions about scope, implementation, and risk management.
- **Cybersecurity Contact Information and Feedback:** Use DOE's published channels for questions and program feedback.

Recommended Small-Business Cybersecurity Resource

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide — NIST Small Business Cybersecurity

NIST SP 800-171 Rev. 3

CISA, Cross-Sector Cybersecurity Performance Goals

Sources

- 15 U.S.C. § 638(vv), Due Diligence Program to Assess Security Risks
- Public Law 119-83, Small Business Innovation and Economic Security Act (Apr. 13, 2026)
- U.S. Department of Energy, Security Risk Management: SBIR/STTR
- SBA, SBIR/STTR Policy Directive / Policies
- CISA, Cross-Sector Cybersecurity Performance Goals
- NIST, Cybersecurity Framework 2.0 Small Business Quick-Start Guide
- NIST SP 800-171 Rev. 3

PLEASE CLICK ON THE FOLLOWING LINKS FOR MORE INFORMATION/TRAINING:

- **SBIR/STTR CS Requirements: Implementation & Evidence Form/ Self-assessment**
- **Risk Rating Information**
- **Learning and Education Resources (LINK TO APPLICANT RESOURCES)**
- **Auditing Information**
- **Cyber Risk Management FAQs**
- **Cybersecurity Contact Information and Feedback**