DOE SBIR/STTR

CYBERSECURITY IMPLEMENTATION & EVIDENCE | APPLICANT GUIDANCE

Protecting Innovation from Research to Commercialization

DOE SBIR/STTR Security Risk Management • Updated October 2026

Implementation & Evidence Form

RELEASE-SPECIFIC EXCEPTION | FY 2025 PHASE II RELEASE 2 APPLIED OFFICE

For this release only, awardees will complete and submit the Implementation & Evidence Form instead of the Cybersecurity Self-Assessment. The SBIR/STTR Office will provide a submission link to all awardees. They are encouraged to consult the Tier 1 and Tier 2 Supplemental Guides found on the 'Applicant Resource Page'. Do not assume this exception applies to other releases without confirmation.

What is the Implementation & Evidence Form?

The DOE SBIR/STTR Implementation & Evidence Form (Please see link below) enables a Small Business Concern (SBC) to report its current cybersecurity practices as part of DOE's security risk review. It helps DOE assess risks to federally funded research, intellectual property, sensitive information, and supporting systems. This review is separate from the scientific and technical merit review.

Review your business environment, including devices, research equipment, cloud services, external IT providers, and sensitive research information. Describe safeguards that are currently implemented, identify gaps accurately, and do not report planned improvements as completed. SBCs may have an opportunity to strengthen their cybersecurity posture.

The form addresses Tier 1 and Tier 2 baseline cybersecurity practices. Review each practice and retain relevant supporting evidence—such as policies, inventories, and configuration records—as directed. The Implementation & Evidence Form and the Cybersecurity Self-Assessment are distinct submissions; follow the instructions for your specific release.

Link to DOE SBIR/STTR Cybersecurity Tiers 1 & 2 Implementation Evidence

Who is responsible for completing and submitting the form?

The SBC selected for an SBIR/STTR award is responsible for the accuracy, completeness, and timely submission of the form. Designate an internal cybersecurity lead to coordinate responses and evidence. The owner, principal investigator, or another authorized representative should verify who may submit through the specified mechanism. An IT service provider or consultant may assist, but accountability remains with the SBC.

Where can I find the form and assistance?

The Implementation & Evidence Form is available on the Applicant Resource Page, along with the Tier 1 and Tier 2 Supplemental Guides, cybersecurity presentations, videos, and other training resources.

When is the Implementation & Evidence Form due?

The applicable DOE funding opportunity and cybersecurity submission instructions determine the deadline. Review the phase, release, and any amendments to confirm whether submission is required with the application

or at another specified point. Allow sufficient time to coordinate with your cybersecurity lead and service providers.

Cybersecurity Self-Assessment

What is the Cybersecurity Self-Assessment?

The DOE SBIR/STTR Cybersecurity Self-Assessment is used to evaluate an SBC's cybersecurity risk. Applicants selected for an SBIR/STTR award must examine their practices and indicate whether the required DOE SBIR/STTR baseline cybersecurity practices are fully implemented before research and development begin. The SBIR/STTR Office reviews the responses and provides a security risk rating. If required practices are not fully implemented, the SBC has an opportunity to implement the remaining practices before the project start date.

Who is required to complete the Self-Assessment?

All FY 2026 SBIR/STTR Phase II awardees are required to complete the Cybersecurity Self-Assessment. Phase I awardees interested in applying for Phase II awards are encouraged to review the assessment and begin implementing the practices.

Where can I find the Self-Assessment?

The Cybersecurity Self-Assessment is available on the Applicant Resource Page, together with Tier 1 and Tier 2 Supplemental Guides, cybersecurity slides, helpful links, and videos.

When is the Cybersecurity Self-Assessment due?

The applicable DOE funding opportunity and cybersecurity submission instructions determine the deadline. Check the phase, release, and any amendments to confirm the exact due date and submission point. Coordinate early with your cybersecurity lead and service providers.

Link to DOE SBIR/STTR TIER 1 Self-Assessment

Link to DOE SBIR/STTR TIER 2 Self-Assessment