The DOE SBIR/STTR Cybersecurity Self-Assessment

The SBIR and STTR Extension Act of 2022 requires agencies to implement and establish a due diligence program to assess the security risks of SBIR/STTR applicants & awardees. In response to this new requirement, the DOE SBIR/STTR Office developed a self-assessment to assess the cybersecurity (CS) business practices of SBIR/STTR Applicants and Awardees. The self-assessment is a subset of CS Performance Goals (CPGs) developed by the CS and Infrastructure Security Agency (CISA) and aligned with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). The self-assessment is due at the time of application submission. Applicants are encouraged to review additional training/guidance for each CPG on our website: SBIR Introduction to Cybersecuri... | U.S. DOE Office of Science(SC) (osti.gov)

NOTE: On the CISA's Checklist it states the 'Recommended Action' for each CPG, however, this has been modified on the SBIR/STTR Self-Assessment to provide additional clarification/guidance for each CPG and has been renamed 'DOE Requirement.'

Cybersecurity Self-Assessment Instructions:

Applicants who possess an active CS Maturity Model Certification (CMMC) Level 2 or 3 meet/exceeds the DOE CS requirement for SBIR/STTR grants. Applicants may opt out of completing the CS Self-Assessment by selecting the applicable CMMC certification level found on the top of the form. **You must also attach a copy of the CMMC Certification to your application.** Applicants who have CMMC Certification Level 1 do not meet the DOE CS Self-Assessment requirement and should complete the self-assessment to be considered for SBIR/STTR awards. For more information regarding CMMC Certification please visit this website: Chief Information Officer > CMMC (defense.gov)

All other applicants please complete the self-assessment and provide a status on your current CS BUSINESS practices. The DOE SBIR/STTR Office will assign a CS Risk Rating which will be used as part of the risk assessment associated with your application.

Select only one of the following responses for each CPG:

- **Implemented:** The small business applicant currently has the CS business practice fully implemented.
- **In Progress:** The CS business practice is not fully implemented; however, actions are being taken to meet full compliance.
- **Not Started:** The small business applicant has not started on the implementation of the CS business practice.

Existing Cybersecurity Certification: Cybersecurity Maturity Model Certification (CMMC) 2.0

- ☐ Level 2
- ☐ Level 3

DOE SBIR/STTR Cybersecurity Self-Assessment:

1.B Organizational Cybersecurity Leadership (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should identify a leader who is responsible and accountable for cybersecurity within an organization. **Related NIST SP 800-53 Control(s):** PM-2	○ Not Started ○ In Progress ◉ Implemented

1.A Asset Inventory (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should create an asset inventory to identify authorized/unauthorized use of any digital service or device that is not formally approved and supported by the IT department, unmanaged/managed assets, and rapidly detect and respond to new vulnerabilities. **Related NIST SP 800-53 Control(s):** CM-8, CM-8(7) CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4	○ Not Started ○ In Progress ◉ Implemented

2.A Change Default Passwords (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should prevent threat actors from using default passwords to achieve initial access or to move laterally in a network. **Related NIST SP 800-53 Control(s):** IA-5(1)	○ Not Started ○ In Progress ◉ Implemented

2.L Secure Sensitive Data (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should protect sensitive information from unauthorized access. **Securing sensitive data entails implementing all CPGs, however, to implement 2.L Secure Sensitive Data Critical CPG requirement, refer to 2.E Separating User and Privileged and 2.D Revoking Credentials for Departing Employees. (The two CPGs are a subset of 2.L and will need to be fully implemented to meet 'Critical' requirement.)** **Related NIST SP 800-53 Control(s):** AC-23, IA-4	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.E Separating User and Privileged Accounts (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised. **Related NIST SP 800-53 Control(s):** AC-2(7), AC-6(9), AC-6(10)	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.D Revoking Credentials for Departing Employees (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** MEDIUM **Complexity:** LOW **DOE Requirement:** The small business should prevent unauthorized access to organizational accounts or resources by former employees. **Related NIST SP 800-53 Control(s):** AC-2(3), AC-2(1)	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.R System Backups (Critical)	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should secure data and reduce the likelihood/duration of data loss during loss of service, delivery, or operations. **Related NIST SP 800-53 Control(s):** CP-9, CP-9(1), CP-9(3)	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.B Minimum Password Strength	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should create and use complex passwords that are harder for threat actors to guess or crack. **Related NIST SP 800-53 Control(s):** IA-5(1)	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.W No Exploitable Services on the Internet	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should identify and monitor all assets, especially public-facing assets, and ensure unauthorized users cannot gain an initial system foothold by exploiting known weaknesses. **Related NIST SP 800-53 Control(s):** CM-7, CM-7(4), CM-7(5)	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.K Strong and Agile Encryption	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should deploy effective encryption to maintain confidentiality and integrity of sensitive data being processed, in transit or at rest. **Related NIST SP 800-53 Control(s):** SC-8, SC-12	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.I Basic Cybersecurity Training	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business' workforce should be trained in cybersecurity and be able to support CS behaviors. **Related NIST SP 800-53 Control(s):** AT-1, AT-2	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

2.H Phishing Resistant MFA	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** MEDIUM **DOE Requirement:** The small business should include additional layer(s) of security to protect assets accounts whose credentials have been compromised. **Related NIST SP 800-53 Control(s):** IA-2(1), IA-2(2)	◯ Not Started ◯ In Progress ◯ Implemented

2.M Email Security	ASSESSMENT
Cost: $$$$ **Impact:** MEDIUM **Complexity:** LOW **DOE Requirement:** The small business should reduce risk from common email-based threats, such as spoofing, phishing, and interception. **Related NIST SP 800-53 Control(s):** AT-2, SC-13, SC-8	◯ Not Started ◯ In Progress ◯ Implemented

2.G Detection of Unsuccessful (Automated) Login Attempts	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should protect assets from automated, credential-based attacks. **Related NIST SP 800-53 Control(s):** AC-7	◯ Not Started ◯ In Progress ◯ Implemented

2.S Incident Response (IR) Plans	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should develop, document, maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios. **Related NIST SP 800-53 Control(s):** IR-1, IR-2, IR-8, IR-9	◯ Not Started ◯ In Progress ◯ Implemented

4.A Incident Reporting	ASSESSMENT
Cost: $$$$ **Impact:** HIGH **Complexity:** LOW **DOE Requirement:** The small business should have security incident reporting procedures to contact an internal incident response team and/or senior management. In addition, the small business should have the CISA, FBI, or local police contact information available to assist with security incidents or understanding the broader scope of a cyberattack. **Related NIST SP 800-53 Control(s):** IR-6, IR-7, IR-4	◯ **Not Started** ◯ **In Progress** ◯ **Implemented**

☐ I acknowledge if selected for an award that DOE may conduct onsite audits to evaluate the implementation of the CPGs to ensure accurate reporting of cybersecurity practices.

☐ I certify that the responses provided are true and accurate.

Name and Title:

Date: