# Proposals for Manufacturing Cybersecurity Program Solicitation

*(No.2024-CAM-04)*

Questions and Answers

Rolling

| | Question | Answer |
|---|---|---|
| 1. | Is software an allowable expense under this solicitation? | Under this program, the only eligible expenses are capital equipment expenses, and software is not eligible. |
| 2. | Are you only considering manufacturers located in Massachusetts for these grants? | Yes, under this program applicants must be Massachusetts-based manufacturers. |
| 3. | Is there a list of non-profit organizations that companies can potentially partner with, including on the third-party cybersecurity assessment? | Given that it is the first year of this program, we do not yet have a list of example partners recipients have leveraged in the past. However, MMAP, a grant program we spun the Manufacturing Cybersecurity Program out of, is structured similarly, and on that [grant's website page](#) we list frequently used non-profit partners, some of whom might be interested in partnering with companies for this program too. For instance, MassMEP runs cybersecurity assessments. |
| 4. | Do you have a restriction on providers for the third-party cybersecurity assessment? | We do not restrict providers of the third-party cybersecurity assessment. We require that assessments be completed within the last 12 months and that applicants submit the summarized results of their assessment, removed of any confidential information, with their application to the program. |
| 5. | Is the 3rd Party assessment covered under the grant? | The third-party cybersecurity assessment, completed within the last 12 months, that we require of applicants cannot be reimbursed with the grant. However, applicants can count fees they incurred completing the assessment as part of their match, as long as they did not use other Massachusetts-state funds for the assessment. |
| 6. | Which cybersecurity standards can manufacturers receive support for pursuing under this program? | This program is designed to support manufacturers pursuing CMMC, ISO 27001, AICPA SOC2, or other mappable, equivalent cybersecurity frameworks. |
| 7. | If we completed a cybersecurity assessment more than one year ago, do we have to | Third party cybersecurity assessments that were completed more than one year ago can be updated |

| | Question | Answer |
|---|---|---|
| | complete a new one, or can we refresh our former assessment? | to meet the needs of the program; an entirely new assessment is not necessary. |
| 8. | When will grants be funded after they are selected? | Applications will be considered on a rolling basis. Once approved, we aim to review and approve applications within approximately two months, after which time contracting between the non-profit partner and MassTech will begin. |
| 9. | For what reasons would an application not be selected? | Proposals will be reviewed, evaluated, and approved upon receipt of a completed proposal that is responsive to the solicitation's requirements and includes all required application components. Mass Tech Collaborative reserves the right to consider such other relevant factors which will be evaluated based on criteria such as:<br><br>■ Projects that advance the recipient's progress towards meeting a cybersecurity standard such as CMMC, ISO 27001, AICPA SOC2, or other mappable equivalent cybersecurity frameworks<br>■ Likelihood that the proposed enhanced cybersecurity infrastructure will enable the Applicant to enter new or existing markets enabled because of enhanced cybersecurity infrastructure<br>■ How the collaboration with a partner will help drive support, business connections and growth<br>■ Contributions to geographic, social, racial and economically equitable outcomes |
| 10. | Are computers eligible for reimbursement under this program? | Yes, computers are eligible for reimbursement, so long as they are treated as capital purchases on applicants' books and aligned with GAAP. |
| 11. | Is penetration testing eligible for reimbursement under this program? | Penetration testing is not eligible for reimbursement under this program, as it is not considered to be capital equipment. However, funds spent on penetration testing can contribute to your 1:1 match requirement. |

|     | Question | Answer |
| --- | --- | --- |
| 12. | Who can conduct our third-party cybersecurity assessment? Can we use our internal IT team? | Third-party assessments, for the purpose of this program, are assessments conducted by a third-party vendor (a non-profit or for-profit vendor that conducts assessments and is separate from your organization), or self-assessments conducted using third-party tools. In the summarized results of your third-party assessment, please indicate which third-party organization or third-party tool you used to conduct your assessment. Given this, your IT team can conduct your assessment if they leverage a third-party assessment tool. |
| 13. | Can upgrades to physical security such as upgrading building alarm hardware systems be covered by this funding? | Upgrades to building alarm hardware systems are eligible for reimbursement under this program. |
| 14. | How do we start the eligibility process? | You will find the details of the program from the program's page here. From there, you will find links to the online application as well as the full solicitation, which contains complete details on the program, and the recording of the information session we hosted in December. |