CYBER-SAFE INCENTIVE PROGRAM

The goal of the Illinois Manufacturing Cyber-Safe Incentive Program is to enhance the cybersecurity measures of small and mid-sized manufacturers (SMMs) in Illinois, with a focus on meeting the NIST 800-171 or CMMC standards. This program is crucial in strengthening the resilience of the supply chain, safeguarding intellectual property, and ensuring business continuity for manufacturers. By doing so, the program aims to promote national security and protect against cyber threats.

Manufacturers who meet the eligibility criteria may receive up to $25,000 in funding to cover documented expenses for cybersecurity implementation and monitoring, such as contractual services, software/hardware costs, and other approved costs. The program aims to award approximately 50 grants, with funding covering no more than 50% of the company's documented expenses between Oct 1, 2022 – May 31, 2023.

Why is this important?

- Small and mid-sized manufacturers are 99% of Illinois manufacturers, representing over 12,000 companies that are cornerstones of Illinois communities across the state.
- Manufacturing experienced over 23% of total cyberattacks in 2021, and 43% of cyberattacks are aimed at small businesses. [1]
- SMMs are lagging in their progress towards strong and mature cyber defenses. This is due to a combination of costs and know-how. It is estimated that only 14% of these businesses are prepared to defend themselves. [2]

[1] https://www.ibm.com/reports/threat-intelligence/

[2] https://www.accenture.com/us-en/insights/cyber-security-index

Eligibility:

- The company must be primarily engaged in the manufacturing and related R&D/ Engineering identified by NAICS codes as validated by Dunn & Bradstreet.
- Funded projects must be for manufacturing establishments in Illinois.
- The company must employ 5 to 250 employees.
- Grant recipients are required to demonstrate proof of a documented assessment of any gaps related to the NIST and/or CMMC standards.
- Grant recipients must provide documentation of expenditures solely related to addressing the results of the gap assessment. The award amount will not exceed 50% of the total project cost. For instance, a company that is granted the maximum award of $25,000 must present evidence of at least $50,000 in expenditures specifically tied to cybersecurity implementation.

Process Steps:

Step 1: Complete the online application by March 31, 2023

Step 2: Eligibility and scoring review

- Virtual meeting with IMEC Specialist, as needed

Step 3: Award decision and notification

Step 4: Reimbursement submission

- Documented gap assessment and expenditures (i.e. – paid invoices) for related implementation and/or monitoring costs. Reimbursements will be up to 50% of documented costs.
- Complete W-9 Form.
- Allow for an on-site visit (at the discretion of IMEC) to verify equipment is on-premises or software is in use.

Step 5: Complete "insight story"

- Share the successes and challenges of cybersecurity implementation for small and mid-sized manufacturers.
- The manufacturer will have final approval of the story.

Step 6: Complete impact survey

- To assess the results in cost savings, investments, sales, and jobs created/retained related to cybersecurity implementation.

Step 7: Reimbursement processed by IMEC

Vouchers <u>can be used</u> to:

- Defray costs related to improving cybersecurity progress tied to an assessment of gaps toward achieving the NIST 800-171 or CMMC standards
- Eligible expenses include consulting services, hardware/software, and supplies

Vouchers <u>cannot be used</u> for ordinary and necessary business expenses or any of the following:

- Expenditures that are related to cybersecurity but not specifically needed to achieve the NIST 800-171 or CMMC standards
- Any expenditure of time by in-house personnel of the applicant
- IMEC services
- General marketing or sales activities
- General business advice, consulting, or basic professional services
- Costs associated with applying for grants and programs
- Entertainment or hospitality costs

To apply for this program, please visit: www.IMEC.org/cybersafe

For additional information, please submit an email to IMEC at Grants@imec.org

MEP National Network

IMEC

Plan. Implement. Excel.