**Project Narrative**

Since [*year*], [*Organization Name*] has provided [*this critical service/core capability*] to [*area name, list or count of cities, counties and/or regions served, approximate total population served*]. Our organization has [*approximate number of employees*] and [number] devices on our network. Our core capability(s) mentioned above, rely on our IT infrastructure [*why is your IT or Operational Technology integral to performing your key operational functions?].*

[*Organization Name*] is applying for this SLCGP funding to [*manage THIS risk. [[1]](#footnote-1) (If you know what your risks are, if not you should be applying to determine your risk), What is the grant for specifically (what equipment/services)? Why do you want to do this? How will it protect your critical assets and the communities/organizations that rely on you?]. [what have you already done to improve your organizations cybersecurity? e.g., training, hired people to manage your environment, used CISA resources, joined MS-ISAC or other ISAC, had consultations, etc*.] Why is this the next logical step or is it the first step?

**Investment Strategy**

[*Describe in narrative form how your project strategy effectively demonstrates the objectives of preventing, preparing for, protecting against, and responding to cyber incidents. Proposals must address closing the gaps in applicants’ identified core capabilities and reducing the overall risk to the community, state or nation. (Refer to the four program objectives and 16 required elements as well as your responses in the gap assessment and any cyber vulnerability or risk assessments performed in the last 12 months.)] [How will this project be sustained i.e., “funded” after the grant period ends?]*

**Collaboration**

[*Regional, statewide or multi- state impact. Describe in narrative form the extent to which the project demonstrates a willingness to collaborate with federal, state, and local governments in efforts to prevent, prepare for, protect against, and respond to acts of cyber-crime and reduce the overall risk to the state or the nation. (also include consultations with similar agencies, city, county, regional, state, federal or private 3rd party entities as well as any DHS, MS-ISAC or CISA services leveraged by your organization to include: Memberships, Training, Exercises, Tabletop Exercises, Information Sharing (ingoing and outgoing, Incident Response etc.)*]

**Budget Narrative**

**Quote, budget table, budget narrative, funding request and match should all sync up.** [*Describe in narrative form your project’s budget plan, demonstrating how it will maximize cost effectiveness of grant expenditures. What is the plan for financial sustainability (how will you maintain the respective services/equipment after the life of the grant)? Are local matching funds available? Will you be doing an in-kind match? Will you be submitting a match waiver?*

**Sustainability Timeline**

*[example]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **2023** | **2024** | **2025** | **After Grant** |
| **SLCGP** | MSP | MFA, Backups, .gov, MSP | Train Personnel (CompTIA, SANs certifications), MSP | MSP, track legacy systems, train personnel |
| **CISA/DHS** | MDBR, PISCES, Nationwide Cybersecurity Review, Cyber TTX | Nationwide Cybersecurity Review, Fusion Center Liaison | Nationwide Cybersecurity Review (NCSR) | Continue NCSR, MS-ISAC, MDBR, PISCES, CISA Cyber Hygiene Program, Cyber TTXs, Fusion Center Liaison |
| **Objectives** | 2 – Understanding Risk | 3 – Equipment and Best Practices | 4 - Training |  |
| **Required Elements** | 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | 5. Adopt and use best practices and methodologies to enhance cybersecurity* Implementation of multi-factor authentication.
* End the use of unsupported/end of life software and hardware that are accessible from the Internet.
 | 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | 12. Leverage cybersecurity services offered by the Department |

**Milestone timeline for individual activities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fiscal Year \_\_\_\_, Q1**  | **Fiscal Year \_\_\_\_, Q2**  | **Fiscal Year \_\_\_\_, Q3**  | **Fiscal Year \_\_\_\_, Q4**  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Impact/Outcomes**

[*Describe in narrative form the solution; describe in detail what will be accomplished by this project. Include what procedures will be implemented, what capabilities will be enhanced, how identified threats and hazards will be mitigated, and the ways in which improvements will be measured/evaluated. Which objectives in the NOFO will be met (1-4)? Which sub-objectives? Which required elements will be met (1-16)?]*

*Defer to application GUIDE, NOFO, and Cross-Sector Performance Goals if you need help.*

1. Refer to the [CISA Cross Sector Cybersecurity Performance Goals](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals) when drafting this document. [↑](#footnote-ref-1)