



- Which mandatory systems, or items, do you currently have in place or fully implemented? Select all that apply:

*Advanced Endpoint Protection (AEP)\* Domain  
Migration Services (Migration to .gov)\*  
Immutable Data Backup and Recovery Testing\*  
Multifactor Authentication Capability (MFA)*

## Part II: Project Details

Which Cybersecurity service will you be perusing with this grant? Select one:

|   |
|---|
| <b>[1]</b>  |
| Advanced Endpoint Protection (AEP)*                         |
| Domain Migration Services (Migration to .gov)*              |
| Immutable Data Backup and Recovery Testing*                 |
| Multifactor Authentication Capability (MFA)*                |
| Albert Sensors  |
| Information Security Awareness Training                     |
| URL/Web/Content filtering                                   |
| Vulnerability Management Services & Scanning                |
| Consulting and Planning Services                            |
| <b>[2]</b>  |
| Converged Endpoint Management (XEM)                         |
| Cyber Security Risk Assessment Services                     |
| DNS Filtering   |
| Email security gateway                                      |
| Enhanced Network Protection - Firewall Services             |
| Identity & Access Management Solutions                      |
| Mobile Device Management (MDM) Solutions                    |
| Penetration Testing Services                                |
| Privileged Access Management (PAM)                          |
| Web Application Firewall (WAF)                              |
| <b>[3]</b>  |
| Application Security Services                               |
| Security Information and Event Management (SIEM) Technology |
| MDR/XDR Solutions   |

Describe the project. What will this project do? Please be as clear and direct as possible in your first paragraph. Supporting details may be provided in the second or third paragraphs.

Have you received quotes for the costs of the items, training, or services described above?

| POETE Areas         |   |
|---------------------|---|
| <b>Planning</b>     | Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information      |
| <b>Organization</b> | Individual teams, an overall organizational structure, and leadership at each level in the structure  |
| <b>Equipment</b>    | Equipment, supplies, and systems that comply with relevant standards  |
| <b>Training</b>     | Content and methods of delivery that comply with relevant training standards  |
| <b>Exercises</b>    | Exercises and actual incidents that provide an opportunity to demonstrate, evaluate, and improve the ability of core capabilities to perform assigned missions and tasks to standards |

**Project Budget Defined by POETE**

|              |    |
|--------------|----|
| Planning     | \$ |
| Organization | \$ |
| Equipment    | \$ |
| Training     | \$ |
| Exercises    | \$ |

Total amount of funds requested in this application: \$

Clearly describe how the project ties to Oregon's SLCGP Cybersecurity Plan.

**Part III: Risk [60 points total]**

*As you consider your project, examine capability gaps to address cybersecurity. What threats, vulnerabilities, and consequences do you face as a result of this gap? Be specific to the service area you selected above.*

**A) Threats [20pts]:** When considering cyber threats, please list and substantiate potential threats against your organization, related organization, network, or cell. Description can include findings from a threat or risk assessment, police report(s), and/or insurance claim(s). Please include dates with supplemental materials.

**B) Vulnerabilities [20pts]:** Please describe the organization's susceptibility to destruction, incapacitation, or exploitation by a cyber attack.

**C) Potential Consequences [20pts]:** Please describe the potential negative effects on the organization's assets, systems, and/or function if damaged, destroyed, or disrupted by a cyber attack because of the identified vulnerabilities.

#### Part IV: Solutions and Services [50pts]

*In this section, compare your solution selected the cybersecurity service list in Part II with the risks identified in Part III.*

- A) Identify the vulnerability (as selected in Section III-B) to be addressed
- B) Describe each proposed activity or investment (solution) to address the vulnerability
- C) For each solution, include the action, item quantity, plan, plan development, and estimated price

| Vulnerability | Solution / Services | Quantity | Total Costs |
|---------------|---------------------|----------|-------------|
|               |                     |          |             |
|               |                     |          |             |
|               | Totals              |          |             |

**Part V: Milestones, Project Management, and Sustainability [20pts]**

Please list at least four milestones and estimated time (number of days, or weeks, or months) required to complete that milestone.

| Milestone | Time to Complete |
|-----------|------------------|
|           |                  |
|           |                  |
|           |                  |
|           |                  |

A) Please describe the measurable outputs and outcomes that will indicate that this investment is successful at the end of the period of performance.

B) Please describe the project team, their contact information, and their roles in completing this project.

C) Please describe how this capability will be maintained.

D) In two or three words, name your project:

Email your application to [SLCGP.admin@oem.oregon.gov](mailto:SLCGP.admin@oem.oregon.gov). Applications will be pulled and reviewed quarterly.

~end~