Maryland SLCGP FAQs
FFY2022

1. **The Committee has created a list of best practices for Maryland Project Categories 1 & 2. What are the definitions for these best practices?**

   The definitions of the best practices are as follows:

- **Asset Discovery/Management** - the capability of mapping and understanding of assets on your network(s). Including understanding which assets or hosts are most critical to protect. Then continually checking those assets for known or potential vulnerabilities and resolving them.
- **Multi-Factor Authentication** - a system that requires more than one distinct authentication factor for successful identification and authentication.
- **End-Point Detection and Response (EDR)** - the capability through tools, personnel or resources, to continuously monitor endpoint activity (e.g. computers, servers, mobile devices) in real time, and to identify and respond to cyber threats or attacks or unauthorized devices, applications and activities and enhance threat detection, response and investigative capabilities.
- **Email Gateway** - an email solution that sits inline on emails' path from the public Internet to the organization's email server. This solution is designed to inspect emails for malicious content and block that content before reaching the organization's system.
- **Security Awareness Training** - training used to help users and employees understand the role they play in helping to combat information security compromises.
- **Firewalls** - a service or tool that filters data traffic on your network or coming into your network with the purpose of blocking cyber threats.
- **Enhanced logging** - a process that encrypts the logs for safe transport to the support administrators. Enhanced logging also provides advanced information in the event log to help administrators troubleshoot issues they may encounter with specific devices (such as USB or video components).
- **Data encryption** - a process/program that translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. This can be applied to data at rest and/or in transit.

- **End of use processes of software and hardware** - stopping the use of unsupported/end of life software and hardware that are accessible from the Internet.
- **Prohibit use of known/fixed/default passwords and credentials** - taking actions to prohibit employees' ability to use known/fixed/manufacturer passwords and credentials.
- **Ensure ability to reconstitute systems (backups)** - testing your organization's ability to correctly reconstitute backups at the determined recovery point objective within your planned recovery time objective.
- **Migration to .gov domain** - the migration of all email addresses and websites to a safe and secure .gov domain.

2. **Do applicants have to use the provided budget narrative and project proposal templates for the application?**

Yes, applicants are required to use the provided templates for their application. If you feel the application is missing something additional you would like to include, you can submit additional attachments with your application.

3. **Will there be an extension process available for applicants that will not be able to meet the project application submission deadline?**

The Committee will generally not accept applications after the deadline. However, the Committee may extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good causes for an extension may include technical problems outside of the applicant's control that prevent submission of the application by the deadline, or other exigent or emergency circumstances.

4. **Are the funding amounts listed in the funding notice the amount we should expect for the entirety of the grant?**

The funding amounts in the NOFO are for FFY2022 only, with a 48-month period of performance ("Year 1"). Updated allocation amounts can be found in the FEMA SLCGP Information Bulletin (IB) 479. Funding will be available in FFY 2023, FFY 2024 and FFY 2025. Each FFY will have its own funding notice, allocation amounts, and application period.

5. **Can eligible entities apply for both the Information Security Officers (ISO) service Program and submit a Sub-grant project proposal?**

   Applicants are eligible to apply for both programs. However, they will only be awarded one.

6. **Do I need to complete a W-9 form as part of my application?**

   If you are applying on behalf of a municipality and local health department, you must fill out and submit a W-9 form as part of your application package. Go to www.irs.gov/FormW9 for instructions and the latest information.

7. **Can I submit multiple applications?**
   Entities are allowed to submit multiple applications if they wish to do multiple projects. To do this entities will need to submit the following documents for each project:
   - Maryland FFY2022 SLCGP Subrecipient Project Proposal Application
   - Appendix E: Measurable Milestones
   - Maryland FFY2022 SLCGP Budget Narrative and Justification Template

   The following documents can be submitted once per jurisdiction:
   - Appendix A: Cybersecurity Capabilities Assessment
   - W-9 (if applicable)