CYBERSECURITY GAP ASSESSMENT

DOWNLOAD THIS FORM PRIOR TO COMPLETING
SUBMIT THE DOWNLOADED AND COMPLETED FORM WITH YOUR APPLICATION PACKAGE

Each grant application submitted for the **State and Local Cybersecurity Grant Program (SLCGP)** should address and mitigate gaps in the applicant's cybersecurity posture. Identifying those gaps is a crucial first step. This form will help you communicate your organization's current posture and what type of project(s) you can apply for under the SLCGP to improve cybersecurity within your organization.

One of the main principals in cybersecurity is defense in depth. This is a continuous process and isn't so much about where you are today, but where you are going. We should all commit to making small improvements each year, knowing that we are better today than we were yesterday, but also that we have a long way to go. OHS is happy to help on this journey in any way we can.

The results of this form will be used for two purposes:

1. Your responses will be provided back to you and you will be able to use the information for your SLCGP application.
2. Responses from all applicants will be summarized and used by OHS to determine the overall state of Hawaii's cybersecurity posture individual attributed responses will not be shared without the express consent of the applicant.

QUESTIONS & CONTACT

Ms. Jimmie L Collins
jimmie.l.collins@hawaii.gov
Chief, Planning and Operations
Hawaii Office of Homeland Security

Mr. Glen Badua
glen.m.badua@hawaii.gov
Chief, Grants Management
Hawaii Office of Homeland Security

First Name

Last Name

Title *(please do not use acronyms)*

Organization *(please do not use acronyms)*

Department *(please do not use acronyms)*

Email provided to you by your organization

Cybersecurity

Do you have anyone in-house or 3rd party managing your IT infrastructure or your cybersecurity? *Select all that apply.*

- ☐ We do NOT have IT/cybersecurity support of any kind.
- ☐ We have an in-house IT manager (full or part time)
- ☐ We have an in-house cybersecurity manager (full or part time)
- ☐ We use a 3rd party service to manage our IT environment
- ☐ We use a 3rd party service to manage our cybersecurity

NOTICE: IF YOU ANSWERED, "WE DO NOT HAVE IT/CYBERSECURITY SUPPORT OF ANY KIND," **DO NOT** COMPLETE THE REMAINDER OF THIS FORM

If you selected one or more of any of the remaining answers, the remainder of this form MUST be completed.

ONLY COMPLETE THE REMAINDER OF THIS FORM WITH INPUT FROM any individual(s) who help manage/ maintain your organization's IT infrastructure and/or cybersecurity.

1. Does your organization (via either in-house employees or a 3rd party) manage all information systems, applications, and accounts associated with your network? *Select all that apply.*

- ☐ No – We don't have any of these
- ☐ Yes – Applying software updates on a schedule
- ☐ Yes – Tracking/phasing out legacy systems
- ☐ Yes – Adding/removing and updating users and user privileges

2. Does your organization (via either in-house employees or a 3rd party) monitor information systems, applications and accounts? *This may be proactive or reactive monitoring. Monitoring includes firewall and endpoint logging and log analysis, having an intrusion detection system (IDS) or an intrusion prevention system (IPS).* ***If any of these are in place choose "Yes"***

- ◯ Yes
- ◯ No

3. Does your organization (via either in-house employees or a 3rd party) manage all information systems, applications, and accounts associated with your network? *Select all that apply.*

- ☐ No – We don't have any of these
- ☐ Yes – we maintain an inventory of our software/ applications
- ☐ Yes – we maintain an inventory of our information systems
- ☐ Yes – we maintain an inventory of our users/accounts

4. Does your organization (via either in-house employees or a 3rd party) have any way to track legacy systems within your network? *Legacy Systems are operating systems, software and/or firmware within your environment that are no longer supported by the manufacturer (updates are no longer available). These could be tracked via a spreadsheet or dedicated software.*

- ◯ Yes
- ◯ No

5. Does your organization (via either in-house employees or a 3rd party) have any means to monitor, audit, and track network traffic and activity? *Monitoring includes firewall and endpoint logging, having an intrusion detection system (IDS) or an intrusion prevention system (IPS).* ***If you have any of these choose "Yes"***

- ◯ Yes
- ◯ No

6. Does your organization (via either in-house employees or a 3rd party) manage all information systems, applications, and accounts associated with your network? *Select all that apply.*

- ☐ No – neither
- ☐ Yes – recurring External Vulnerability Scan
- ☐ Yes – recurring Internal Vulnerability Scan systems

7. Have you implemented multi-factor authentication on remote systems and systems that house PII or other sensitive/ mission critical information?

- ◯ Yes
- ◯ No

8. Does your organization (via either in-house personnel or a 3rd party service) perform firewall or endpoint logging and/or analysis of those logs?

- ◯ No
- ◯ Yes – logs and log analysis for both
- ◯ Yes – logs and log analysis for one but not the other
- ◯ Yes – logs for both
- ◯ Yes – logs for one but not the other

9. Do you (either via in-house personnel or a 3rd party service) encrypt data at rest or in transit? *Select all that apply.*

- ☐ No – neither
- ☐ Yes – encrypt some while at rest
- ☐ Yes – encrypt all while at rest
- ☐ Yes – both
- ☐ Yes – encrypt some while in transit
- ☐ Yes – encrypt all while in transit

10. Do you have any of the following password security procedures in place? *Select all that apply.*

- ☐ No/none
- ☐ Passwords must be changed on a recurring schedule
- ☐ Promote or provide password managers
- ☐ Multi-Factor Authentication
- ☐ Prohibit use of known/fixed/default passwords
- ☐ Provide password training

11. Do you have any of the following means of backing up data within your organization? *Select all that apply.*

- ☐ No backups
- ☐ Offline backup
- ☐ Internal backup
- ☐ Cloud backup
- ☐ Offsite backup

12. Does your organization currently have a hawaii.gov or other .gov email address?

- ◯ No
- ◯ Yes (hawaii.gov)
- ◯ Yes (.gov)

13. Has your organization completed any of the following? *Select all that apply.*

- ☐ General Cybersecurity Roles/Responsibilities Identified
- ☐ Completed Continuity of Operations Plan
- ☐ Completed Acceptable Use Policy
- ☐ Completed a Business Impact Analysis
- ☐ Completed Cybersecurity Policy

14. Has your organization ever participated in a cyber tabletop exercise (TTX)?

- ◯ No/I don't know
- ◯ Yes – 1 cyber TTX
- ◯ Yes – 2-3 cyber TTX
- ◯ Yes – we do annual cyber TTXs

15. Is your organization currently a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC)?

- ◯ Yes
- ◯ No/I don't know

16. Have, or do you plan to, use any of the Cybersecurity and Infrastructure Security Agency (CISA) resources listed below? *Select all that apply.*

- ☐ Consultation(s)
- ☐ Vulnerability/Risk Assessment
- ☐ External Vulnerability Scanning/Reporting Web
- ☐ Application Vulnerability Scanning
- ☐ CISA's Known Exploited Vulnerabilities Catalog
- ☐ Public Infrastructure Security Cyber Education System (PISCES)

17. Have you spoken with or received consultation from any of the following regarding cybersecurity best practices? *Select all that apply. **Implementing cyber security standards such as NIST 800-171 or ISO/IEC 27001 are often considered best practices.*

- ☐ CISA
- ☐ Entities similar to mine
- ☐ Fusion Center
- ☐ National Guard
- ☐ Neighboring cities
- ☐ Private Contractor
- ☐ Other:

18. Utilizing DHS/CISA resources is a key element to the SLCGP. Please list any cybersecurity courses either you or your organization have attended within the last 12 months. (e.g. AWR383 Cybersecurity Risk Awareness for Officials and Senior Management, MGT384 Community Preparedness for Cyber Incidents)? *You may include non-DHS/CISA courses as well, but please enter the training in the following format:* ***[Agency], [Course Title] [Month, Year].***