CYBER HYGIENE

Authorization to Conduct Continuous Scans of Public-Facing Networks and Systems

The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS), under authority of Title XXII of the Homeland Security Act (6 U.S.C. § 651 et seq., esp. 6 U.S.C. § 659) would like to gain authorization from Organization Name Here (Org Acronym) to conduct continuous network and vulnerability scanning of Org Acronym's publicly accessible networks and systems.

The goals of these activities are to:

1. Catalog your organization's publicly accessible networks and systems, including services running and version/patch levels
2. Identify vulnerabilities on your organization's publicly accessible networks and systems
3. Identify potential configuration issues with your organization's public facing networks and systems
4. Maintain tactical awareness of the operational risks and cyber health of individual entities
5. Inform the government's common operational view of cyberspace
6. Integrate relevant information, analysis, and vulnerability assessments, in order to identify priorities for protective and support measures regarding potential or actual threats
7. Provide "early warning" of specific, actionable vulnerabilities to your organization

CISA activities will originate from IP addresses or other identifiers that will be made known to your organization.

Scanning will be openly attributable to the authorized scanning source, and should be detected by your organization's network monitoring solutions. Data will be sent to your organization's networks and systems corresponding to the public facing IP addresses, domain names, or other identifiers provided by your organization for scanning. The process has been designed to be as unobtrusive as possible: scheduling, intensity and frequency have been carefully planned to minimize the possibility of service disruption.

Activities under this authorization will be limited to scanning; no attempts to connect to your organization's internal network, penetrate your organization's systems, or monitor your organization's network traffic will be made under this authorization.

If a third-party, such as a cloud service provider, operates or maintains your networks or systems to be scanned pursuant to this authorization, your organization will ensure compliance with any notification or authorization requirement that such third party may impose on external vulnerability scanning services. If your organization is informed that any such third party prohibits external vulnerability scans, you will promptly notify the CISA point of contact listed below.

In a separate appendix to this authorization please provide the following information: the point of contact for activities performed under this authorization; an email address for the delivery of reports; identification information for your organization's networks and systems to be scanned pursuant to this authorization; and any other relevant information. Your organization may provide updates to this information from time to time, in writing, using an updated appendix or other method. Your organization must promptly update CISA of changes to the identifying information used to scan your networks and systems pursuant to this authorization.

CISA acknowledges that this authorization may be withdrawn at any time for any reason.

The CISA Point of Contact for this activity can be reached at vulnerability_info@cisa.dhs.gov. All notifications, updates, or other communications regarding this authorization and any related activity should be sent to this CISA Point of Contact.

By signing below, you agree to the following:

- You have authority to authorize scanning of the networks and systems submitted pursuant to this authorization;
- You authorize CISA to conduct the scanning activities described above;
- You agree to promptly update CISA of changes to the information used to identify the networks and systems to be scanned pursuant to this authorization;
- You agree to comply with any notification or authorization requirement that any third-party that operates or maintains your networks or systems may impose on external vulnerability scanning services, notifying CISA if external scanning is later prohibited;
- You accept that, while CISA teams will use their best efforts to conduct scans in a way that minimizes risk to your organization's systems and networks, the scanning activities described above create some risk of degradation in performance to your organization's systems and networks;
- You acknowledge that CISA provides no warranties of any kind relating to any aspect of the assistance provided under this authorization; and
- You are authorized to make the above certifications on your organization's behalf.

Signature: _____

Name: Name of Authorizing Official **Date:** _____

Title: Title of Authorizing Official

Email: Email of Authorizing Official **Phone:** _____

Entity: Organization's Name Here

City: City **County:** County **State:** State

Country: Country

Appendix A

Authorization to Conduct Continuous Scans of Public-Facing Networks and Systems

Org Acronym _____ *provides the following information to facilitate the authorized scanning activities:*

Please provide a **technical point of contact** at Org Acronym _____ for the CISA team to follow-up with:

Name: Name of Technical POC 1

Email: Email Address for Technical POC 1

Phone: Phone Number for Technical POC 1

Optional secondary **technical point of contact**:

Name: Name of Technical POC 2

Email: Email Address for Technical POC 2

Phone: Phone Number for Technical POC 2

We recommend your organization **create/use a distribution list** email address to receive our reports. This allows your organization to manage the recipients of our report. *We will only deliver reports to a single address.*

Distro email: Email address we send your reports to

Your report will be encrypted with a password which we will provide to you. **How would you like this password delivered** (select one)?

Email @

☐ Tech POC

☐ Distro POC

When should scans begin? (e.g., as soon as possible, or *time*, Eastern @ *mm/dd/yyyy*)

Requested Start Date _____

Identification of Your Public-Facing Networks and Systems:

Enter your organization's **internet-facing, static IPv4 addresses** to be vulnerability scanned in one of the following formats: CIDR notation (e.g. x.x.x.0/24), IP range (e.g. x.x.x.1-x.x.x.200), or individual IPs (e.g. x.x.x.1) with one entry per line:

Example:
1.2.3.5
1.2.3.22-1.2.3.25
1.2.3.40/30