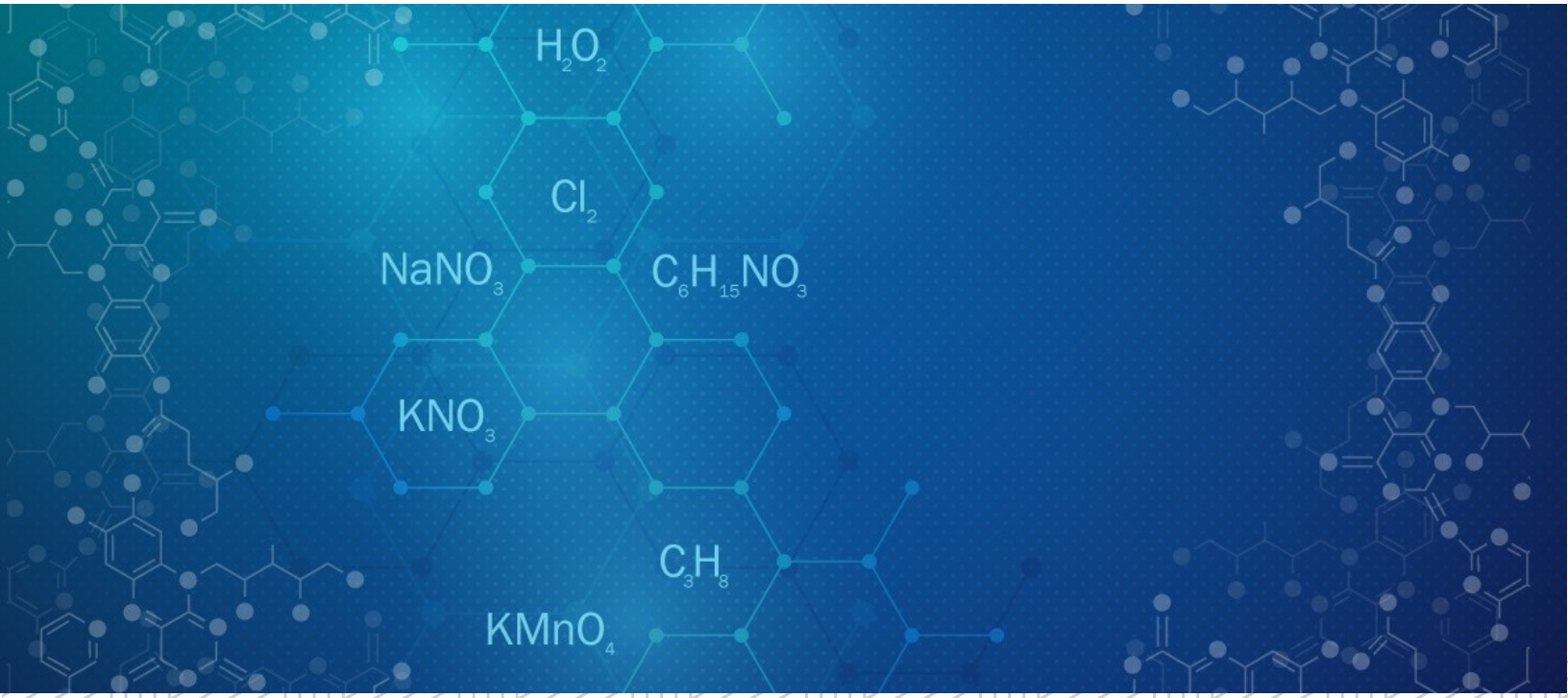

CHEMLOCK SERVICE REGISTRATION AND PREPERATION INSTRUMENT

Cybersecurity and Infrastructure Security Agency

1. Paperwork Reduction Act Statement

In accordance with the Paperwork Reduction Act, no one is required to respond to a collection of information unless it displays a valid Office of Management and Budget (OMB) Control Number. The valid OMB Control Number for this information collection is 1670-NEW. The time required to complete this information collection is estimated to average 3.17 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

2. Privacy Notice

Authority: 6 U.S.C. 652(c)(5) (authorizing CISA to provide analyses, expertise, and assessments to critical infrastructure owners and operators upon request) authorizes the collection of this information.

Purpose: This instrument collect information necessary to perform the requested ChemLock-related service(s).

Routine Use: The Personally Identifiable Information (PII) you provide will be used by and disclosed to DHS personnel, contractors, or other agents, including but not limited to other Federal, state, and local officials; and used to contact the submitter and conduct any administrative follow up actions required to administer the ChemLock program.

Disclosure: Providing this information is **voluntary**. However, failure to provide any of the information requested may limit participation in the program.

3. ChemLock Service Registration and Preparation

This instrument uses verbal conversation, emails, text fields, selection from a drop down menu, check boxes, or similar means to collect the following and similar information. The instrument may also collect follow information to review via email or uploads into a Microsoft tool suite application(s):

Security Consultation / Technical Consultation / Onsite Assessments and Assistance

- Do you have a security plan?
    - If so, may we review the document?
- Have you had a previous assessment or security vulnerability analysis conducted?
    - If so, may we review the document?

- Details of a facility's security personnel
- Dates and times for visit
- Specific security concerns of the facility

To be asked twice at each facility (pre/post baseline):

- Critical detection measures and identified vulnerabilities
- Critical delay measures and identified vulnerabilities
- Critical response measures and identified vulnerabilities
- Critical cyber security measures and identified vulnerabilities
- Critical policies, procedures, and resources and identified vulnerabilities
- Explain the facility's threat and risk assessment efforts, if applicable
- Whether the facility has identified all potential vulnerabilities in their current security posture that require planned improvements in order to meet the applicable Risk Based Performance Standards
- Crisis management plan
- Emergency response plan
- Agreement with external responders (e.g., security or emergency first responders)
- External responders participating in the exercise
- Previous exercise history
- Inventory of emergency response equipment

Regarding cyber assets, the instrument will collect, on a voluntary basis, the following information when the facility identifies a Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Process Control Systems (PCS), or Industrial Control Systems (ICS):

- Provide details on the system(s) that controls, monitors, and/or manages small to large production systems as well as how the system(s) operates.
- If it is standalone or connected to other systems or networks and document the specific brand and name of the system(s).

Risk Assessment

- Information about a facility's chemical holdings:
    - Quantity(ies) of dangerous chemical(s)
    - Concentration of dangerous chemical
    - Storage vessel(s) for dangerous chemical(s)
    - Safety Data Sheet(s) (SDS) for dangerous chemical(s)
- Chemical security and cybersecurity trainings that facility has taken from CISA or other entities