State of Maryland Cybersecurity Action Plan for Water and Wastewater Systems

Prepared by the Maryland Department of the Environment on behalf of the Moore-Miller Administration

June 28, 2024

Wes Moore
Governor

Aruna Miller
Lieutenant Governor

Serena McIlwain
Secretary

Suzanne Dorsey
Deputy Secretary

State of Maryland Cybersecurity Action Plan for Water and Wastewater Systems
June 28, 2024

Executive Summary

The Maryland Cybersecurity Action Plan for Water and Wastewater Systems aims to address critical cybersecurity vulnerabilities within Maryland's water and wastewater infrastructure. This initiative is driven by the urgent need to protect these essential systems from increasingly sophisticated cyber threats, as outlined by recent federal advisories, the Modernize Maryland Act of 2022 (HB1205)[1], and in direct response to the letter from the White House dated March 21, 2024.[2]

The plan’s primary goal is to mitigate high-risk cybersecurity gaps quickly and effectively while setting a foundation for long-term resilience strategy. The increasing frequency and severity of cyberattacks on water and wastewater systems underscore the necessity for immediate action. By leveraging both state and federal resources, this plan seeks to safeguard the public from disruptions to critical water services.

Coverage and Applicability

This plan focuses on "covered systems"—those serving over 3,300 people or utilizing Operational Technology (OT) thus targeting the facilities with the highest potential impact on public health and safety if compromised. The State currently lacks the authority to require all covered systems to address cybersecurity. MDE intends to seek the authority to require all covered systems to perform routine cybersecurity assessments and develop and implement risk mitigation and emergency response plans.

Key Actions

1. **Cybersecurity Assessment for Covered Systems-** Compile a list of covered systems by September 1, 2024, notify systems of their obligations by October 1, 2024, and provide guidance for conducting assessments aligned with the NIST Cybersecurity Framework (CSF).

[1] Modernize Maryland Act of 2022, https://mde.maryland.gov/programs/water/water_supply/Documents/Modernize%20Maryland%20Act%20of%202022%20Guidance.pdf

[2] Letter to Governors on Water Systems Cybersecurity Action Plan, March 28, 2024

2. **Development of Risk Mitigation Plans -** Develop and implement plans within two months of identifying significant vulnerabilities. Include a schedule of specific actions, responsible personnel, and funding sources.

3. **Emergency Response Preparedness -** Integrate cyber response into Emergency/Incident Response Plans by July 1, 2025.

4. **Follow up on Compliance -** Regularly follow up with covered systems to ensure the effective implementation of risk mitigation and emergency response plans and to update them as needed.

5. **Plant staff Cyber Hygiene Training -** Create a routine training requirement for all operators and superintendents by December 2024. Require all operators and superintendents to attend cyber hygiene training during the operator certificate renewal process.

6. **Coordination, Training and Outreach -** Foster coordination among state, federal, and local agencies. Provide ongoing training opportunities and updated resources to water and wastewater systems and encourage participation in information-sharing networks.

Introduction

In the face of increasing cyber threats, the security of Maryland's water and wastewater systems is a critical priority. These systems serve millions of residents and are vital infrastructure. However, modern water and wastewater operations are vulnerable to cyberattacks that can disrupt services and pose significant risks to communities.

To respond to these challenges, the Maryland Department of the Environment (MDE) has developed a cybersecurity plan targeting "covered systems"—those that serve over 3,300 people or utilize Operational Technology (OT). By focusing on these systems, the plan aims to protect the facilities that, if compromised, could have the most substantial impact on public health and safety.

This document describes Maryland's cybersecurity initiatives, detailing the criteria for covered systems, the state's authority and approach to cybersecurity assessments, and the key actions necessary to enhance the resilience of water and wastewater infrastructure. It also provides an overview of previous cybersecurity efforts and the regulatory framework supporting these initiatives.

By implementing these measures, Maryland seeks to establish a robust and coordinated approach to safeguarding its critical water and wastewater systems, ensuring their continued reliability, resiliency and security in the face of evolving cyber threats.

Coverage and Applicability

Covered Systems

The phrase "covered systems" in Maryland refers to any water or wastewater system that meets ***either*** of the following criteria:

- **Systems Serving Over 3,300 People**: Systems serving a larger population have a greater potential impact on public health and safety in the event of a cybersecurity incident. By including these systems, the plan aims to prioritize resources and efforts on those facilities that, if compromised, could affect a significant number of residents.
- **Systems Utilizing Operational Technology (OT):** Operational Technology refers to hardware and software that detects or causes changes through direct monitoring and control of physical devices,

processes, and events. Systems using OT are often more complex and interconnected, making them more vulnerable to sophisticated cyberattacks. Ensuring these systems are secure is critical for maintaining the integrity and functionality of essential water and wastewater services.

By focusing on systems that serve over 3,300 people and those using OT, the plan targets facilities that have the highest potential impact on public health and safety.

State Authority to Require Cybersecurity Assessments

Currently, the State of Maryland lacks the authority to mandate cybersecurity assessments, risk mitigation plans, and incident response plans for all water and wastewater systems. While progress can be made through voluntary measures, this approach risks creating an uncoordinated patchwork of inconsistent plans across the state. MDE intends to seek authority to require "Covered Systems" to:

1. conduct routine cybersecurity control assessments every three years
2. develop and implement risk mitigation plans to address significant vulnerabilities identified in these assessments
3. integrate cyber incident response procedures into existing emergency response plans.

Should regulatory authority not be granted, the plan will proceed on a voluntary basis.

Cybersecurity control assessments are governance evaluations focused on ensuring an organization's security controls align with defined standards and effectively mitigate risks. These assessments, guided by frameworks like the NIST Cybersecurity Framework (CFS), involve a comprehensive review of policies, procedures, and technical implementations to verify compliance with best practices and regulatory requirements. These assessments help identify gaps and weaknesses in the security posture. The insights gained drive risk mitigation plans, including updating or implementing new controls, to address deficiencies and enhance overall cybersecurity governance and defense.

Notably, MDE will not require the submission of these plans to avoid additional cybersecurity risks; instead, systems will provide written certification that the requirements have been fulfilled (or not) and meet the State Minimum Cybersecurity Standards (or not).

Key Actions

The following key actions section outlines the specific measures that will be implemented to enhance the cybersecurity of Maryland's water and wastewater systems. These actions focus on conducting risk assessments, developing mitigation plans, implementing security controls, ensuring emergency preparedness, and leveraging available resources for comprehensive protection and resilience.

1. Cybersecurity Assessment for Covered Systems

Certain water and wastewater utilities in Maryland have already been required to address cybersecurity under various Federal and State laws. However, many smaller utilities within Maryland were not subject to these earlier requirements, but may still have cyber vulnerabilities.

MDE will do the following:

1. **Generate a List of Covered Systems:**

   By September 1, 2024, MDE will compile a list of all covered systems based on the criteria of customer size and operational technology use.

2. **Conduct Outreach:**

   By October 1, 2024, MDE will send formal notification letters to these systems, informing them of their obligations under the new cybersecurity requirements, if in place. Otherwise the assessments will be requested. For systems that have not recently completed an assessment, an assessment will be requested to be completed, either within six months of the notification or based on a timeline set in the requirement.

3. **Provide Guidance:**

   1. MDE will supply systems with guidance documents and resources from EPA, CISA, and AWWA, including templates and checklists to conduct thorough cybersecurity control assessments.
   2. Guidance will require that the assessment meet the State of Maryland’s Minimum Cybersecurity Standards, which align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
   3. MDE will strongly recommend that water systems implement ongoing cyber security vulnerability scanning. CISA performs this function free to systems that enroll in their service (CISA Cyber Hygiene Services).

2. Risk Mitigation Plan for Covered Systems

Covered water and wastewater systems would also be required to develop and implement a risk mitigation plan if significant cybersecurity vulnerabilities are identified during a cyber assessment. The risk mitigation plan is to be developed within two months of completing the cybersecurity assessment. A risk mitigation plan includes a schedule of specific actions and identifies responsible personnel and funding sources.

MDE will contact each covered system to identify those systems that require a risk mitigation plan, and to determine whether a plan is in place and being implemented.

3. Emergency/Incident Response Plan for Covered Systems

As part of its October 1 outreach, MDE will direct covered water and wastewater utilities to incorporate cyber response into their Emergency/Incident Response Plans by July 1, 2025.

This plan will assist a system to prepare for, respond to and recover from a cyber incident. It will define roles and responsibilities clearly and offer guidance on essential activities. Additionally, it will incorporate a roster of key personnel and a schedule for periodically exercising the plan. Water systems in Maryland are already required to have up-to-date Emergency Response Plans.

4. Follow up with each system on Risk Mitigation and Incident Response Plans

By December 2024, standardized methods will be developed to review the status of cybersecurity practices during routine inspections at covered water and wastewater systems. Staff will review compliance with triennial cybersecurity assessments, that utilities are implementing a risk mitigation plan, if necessary, and that systems are maintaining and utilizing up-to-date emergency response or incident response plans. The review of cybersecurity assessments and risk mitigation plans will only occur on site at facilities. If a covered system is deficient in any of these areas, MDE staff will request that the utility develop a plan for addressing those deficiencies and direct the system to available resources.

With current resources and inspection frequency, these inspections occur over a 3 to 5 year period for drinking water systems and every 1 to 3 years for wastewater systems.

- Cybersecurity will have been included in all inspections for large drinking water systems by December 2027 and small systems by 2029 and tracked as part of key performance indicators.
- MDE will include cybersecurity in wastewater inspections for large Wastewater Treatment Plants by December 2025 and small systems by December 2027 and tracked as part of key performance indicators.

5. Operator and Superintendent Cyber Hygiene Training

By December 2024, MDE will create a routine cyber hygiene training requirement for all water and wastewater operators and superintendents through its Board of Waterworks and Waste Systems Operators. Basic cyber security practices can prevent the vast majority of cyber attacks, and this training will provide basic knowledge to those operating water and wastewater utilities. Cyber risks are prevalent in everyday tasks and knowing when to spot those risks and report them is crucial to protecting systems and critical infrastructure.

Coursework may be similar to the free training offered through CISA in its Cybersecurity Awareness Program through the Federal Virtual Training Environment (FedVTE).

MDE is also investigating approaches to train elected officials who manage water or wastewater systems on cybersecurity, such as the Academy for Excellence in Local Governance Program, run by the Maryland Municipal League (MML).

6. Coordination, Training Exercises, and Outreach

Preparing for and responding to cyber threats will require a whole-of-government approach, and regular coordination among state, federal, and local agencies. In particular, it will require regular coordination and collaboration between MDE, the Department of Information Technology (DoIT), the Maryland Department of Emergency Management (MDEM), the Governor's Office of Homeland Security, EPA, CISA, and Public Water Systems.

MDE intends to become a central resource for water and wastewater systems to stay informed of cybersecurity resources, risks, prevention, practices, and response to attacks. Starting in 2024, MDE will schedule regular coordination meetings with the MDEM and DoIT. The Maryland Local Cybersecurity Collaborative (MLCC) formed a Water/ Wastewater Cybersecurity Subcommittee in 2024, and has members from DoIT, CISA, the Maryland Environmental Service, and MDE.

- MDE will coordinate with DoIT, MDEM, EPA, and CISA in 2024 to provide regular training to water and wastewater systems via tabletop exercises, conference presentations, and webinars.
- MDE will coordinate with the Maryland Rural Water Association to provide technical assistance to utilities.
- MDE will encourage utilities to participate in information-sharing networks, such as the Homeland Security Information Network - Critical Infrastructure (HSIN-CI), MD-ISAC and WaterISAC.
- MDE will develop cybersecurity communication material for water and wastewater systems, and will update its website to include links to various available resources to assist utilities with cybersecurity.

Previous Cybersecurity efforts

America's Water Infrastructure Act (AWIA) of 2018

America's Water Infrastructure Act (AWIA) of 2018 requires community water systems serving over 3,300 users to assess and certify their risks and emergency response plans to the EPA every five years. The Act emphasizes utilizing available resources, such as free assessments and technical assistance from the EPA, and aims to enhance the resilience and security of Maryland's critical water infrastructure against cyber threats

Modernize Maryland Act of 2022 (HB1205)

The Modernize Maryland Act of 2022 (HB1205) mandates that all public or private water and wastewater systems in Maryland serving 10,000 or more users and receiving state financial assistance must conduct a cybersecurity vulnerability assessment, develop a cybersecurity plan if necessary, and submit a report of their findings and any statutory recommendations to the General Assembly by December 1, 2023. This legislation also aligns Maryland wastewater systems with the requirements of AWIA. Due to the Modernize Maryland Act, water systems serving over 85 percent of Marylanders have performed cybersecurity assessments

Maryland's Critical Infrastructure Cybersecurity Act of 2023

Maryland’s Critical Infrastructure Cybersecurity Act of 2023 requires the 22 privately-owned water and wastewater systems regulated by the Public Service Commission to perform third-party cybersecurity assessments every two years and adopt and implement cybersecurity standards. It also required these utilities to report all cybersecurity incidents to the State Security Operations Center.

Cybersecurity Breach Reporting

Md. Code Regs. 20.06.01.05 requires that all utilities must report confirmed cybersecurity breaches involving a smart grid system, information technology system, or operations technology system to a designated representative of the Commission within one business day of confirmation. The report must exclude energy/electric infrastructure information as defined by 18 CFR § 388.113, unless law enforcement advises against it to avoid compromising an investigation.

Attachment A - EPA Links to Cybersecurity Information

- Guidance on assessing if a water or wastewater system has operational technology
- Free self assessment tool Water Cybersecurity Assessment Tool (WCAT)
- Third party, no-cost Water Sector Cybersecurity Evaluation
- Cybersecurity Help Desk
- Templates and guidance on emergency response plans
- Cybersecurity Incident Action Checklist
- Community Water System Emergency Response Plan Template and Instructions
- Wastewater Utility Emergency Response Plan Template and Instructions
- Water Resilience Training
- Vulnerability Self Assessment Tool
- CISA/EPA/FBI Incident response Guide
- Cyber Incident Reporting Process

CISA Links

- Cyber Hygiene Services

Other Links

- FEMA's courses from the Emergency Management Institute
- NIST's Guide to Operational Technology Security

Attachment B - March 28, 2024 Letter to the Governor

THE WHITE HOUSE
WASHINGTON

March 28, 2024

Dear Governor,

Thank you to your homeland security, health, and environmental officials for participating in the March 21, 2024 call regarding water system cybersecurity. As outlined in the recent letter you received from Assistant to the President for National Security Affairs Jake Sullivan and U.S. Environment Protection Agency (EPA) Administrator Michael Regan, your partnership is essential as we work together to address the risks that cyberattacks pose to the nation's drinking water and wastewater systems.

We have seen multiple cyber threat actors, both nation-state and criminal, target the water and wastewater sector. The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation, and EPA have released Cybersecurity Alerts and Advisories on the threats we face, and many states actively engage with their water sector systems to promote cybersecurity. But many water and wastewater systems continue to suffer from significant gaps in their existing cybersecurity practices that leave them vulnerable to potentially disabling attacks. As a result, the cyber threat continues to present an imminent and substantial risk.

I write today to ask for your help. On behalf of the National Security Advisor, we are asking each state to prepare an action plan that outlines its plan to mitigate the most significant cybersecurity vulnerabilities in the state's water and wastewater systems. The goal for these action plans is to eliminate high-risk cybersecurity gaps—gaps which often can be corrected quickly and easily (e.g., changing default passwords in operational technology)—while ensuring that all water and wastewater sector systems continue or embark on a path to cyber risk reduction and resilience. Due to the need to address these risks quickly, we ask that these plans be completed in 90 days.

Attached to this letter is guidance on suggested content for states to include in the water sector cybersecurity action plans. States are welcome to tailor their plans to fit current programs, capabilities, priorities, and water system oversight structures. The crucial essence of the plan, however, should be your state's approach to identify and address the cybersecurity vulnerabilities that create the highest risk to your water and wastewater systems.

I also want to share with you several resources to help develop and implement your plan. In addition to the Department of Homeland Security's Cybersecurity and Infrastructure Security Advisors in your state, the EPA and CISA offer free guidance, tools, training, resources, and technical assistance. Examples include conducting cybersecurity risk assessments at water and wastewater systems, developing risk mitigation plans, and providing near real-time technical assistance with implementing cybersecurity controls. Private water sector associations, including the American Water Works Association, the National Rural Water Association, and the Water Information Sharing and Analysis Center, among others, also provide cybersecurity tools and technical support.

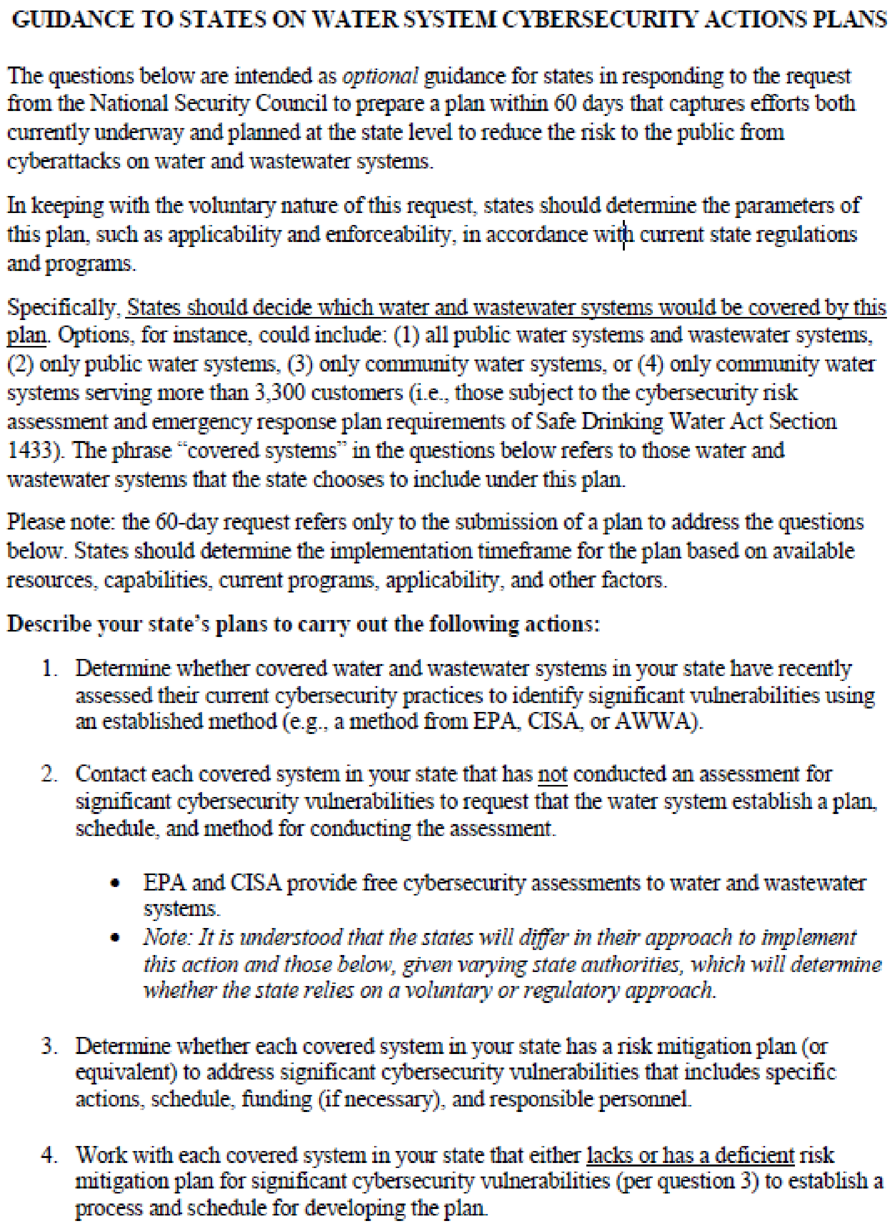
As EPA Deputy Administrator Janet McCabe has stated, EPA is, as part of its National Enforcement and Compliance Initiative, conducting inspections of community water systems, and EPA will continue to take enforcement actions where needed. EPA intends to increase its inspection activity to protect against any imminent and substantial endangerment.

When your state completes its water and wastewater sector system cybersecurity action plan (or if you have questions regarding the preparation of this plan, access to support resources for water system cybersecurity, or other concerns related to this effort), please send it to the National Security Council's Director for Critical Infrastructure Cybersecurity, Jon Murphy, at Jonathan.S.Murphy@nsc.eop.gov. In keeping with the requested 90-day development timeframe, please share these plans by Friday, June 28.

Thank you for your vital support and partnership to ensure that these systems take the necessary steps to address this risk. If you or your staff would like to engage directly on any aspect of this request, please contact me at Anne.Neuberger@nsc.eop.gov.

Anne Neuberger
Deputy Assistant to the President and
Deputy National Security Advisor
Cyber and Emerging Technologies

Attachment C - Guidance Provide to States



GUIDANCE TO STATES ON WATER SYSTEM CYBERSECURITY ACTIONS PLANS

The questions below are intended as *optional* guidance for states in responding to the request from the National Security Council to prepare a plan within 60 days that captures efforts both currently underway and planned at the state level to reduce the risk to the public from cyberattacks on water and wastewater systems.

In keeping with the voluntary nature of this request, states should determine the parameters of this plan, such as applicability and enforceability, in accordance with current state regulations and programs.

Specifically, States should decide which water and wastewater systems would be covered by this plan. Options, for instance, could include: (1) all public water systems and wastewater systems, (2) only public water systems, (3) only community water systems, or (4) only community water systems serving more than 3,300 customers (i.e., those subject to the cybersecurity risk assessment and emergency response plan requirements of Safe Drinking Water Act Section 1433). The phrase "covered systems" in the questions below refers to those water and wastewater systems that the state chooses to include under this plan.

Please note: the 60-day request refers only to the submission of a plan to address the questions below. States should determine the implementation timeframe for the plan based on available resources, capabilities, current programs, applicability, and other factors.

Describe your state's plans to carry out the following actions:

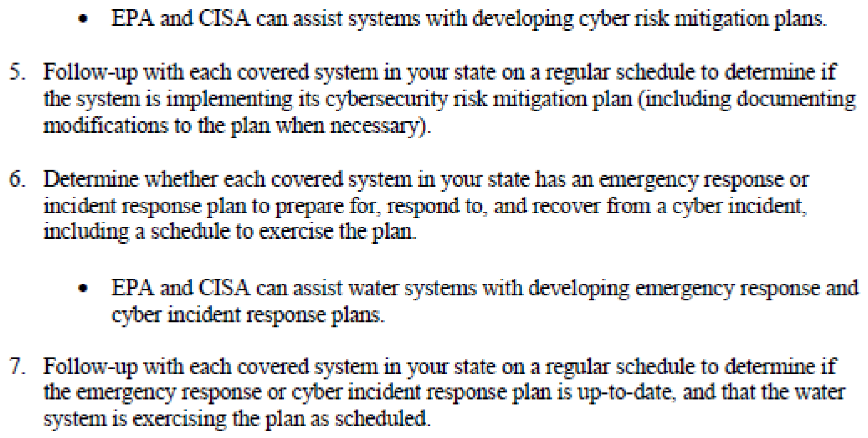
1. Determine whether covered water and wastewater systems in your state have recently assessed their current cybersecurity practices to identify significant vulnerabilities using an established method (e.g., a method from EPA, CISA, or AWWA).

2. Contact each covered system in your state that has not conducted an assessment for significant cybersecurity vulnerabilities to request that the water system establish a plan, schedule, and method for conducting the assessment.

   - EPA and CISA provide free cybersecurity assessments to water and wastewater systems.
   - *Note: It is understood that the states will differ in their approach to implement this action and those below, given varying state authorities, which will determine whether the state relies on a voluntary or regulatory approach.*

3. Determine whether each covered system in your state has a risk mitigation plan (or equivalent) to address significant cybersecurity vulnerabilities that includes specific actions, schedule, funding (if necessary), and responsible personnel.

4. Work with each covered system in your state that either lacks or has a deficient risk mitigation plan for significant cybersecurity vulnerabilities (per question 3) to establish a process and schedule for developing the plan.



- EPA and CISA can assist systems with developing cyber risk mitigation plans.

5. Follow-up with each covered system in your state on a regular schedule to determine if the system is implementing its cybersecurity risk mitigation plan (including documenting modifications to the plan when necessary).

6. Determine whether each covered system in your state has an emergency response or incident response plan to prepare for, respond to, and recover from a cyber incident, including a schedule to exercise the plan.

    - EPA and CISA can assist water systems with developing emergency response and cyber incident response plans.

7. Follow-up with each covered system in your state on a regular schedule to determine if the emergency response or cyber incident response plan is up-to-date, and that the water system is exercising the plan as scheduled.