Data Quality Record for Long-Term Performance Goals

Long-Term Performance Goal Text: By September 30, 2026, EPA will be in full compliance with the five high-priority directives in *Executive Order 14028 - Improving the Nation's Cybersecurity*.

Corresponding Annual Performance Goals:

- Percentage of EPA applications in compliance with multifactor authentication requirements.
- Percentage of EPA data at rest in compliance with encryption requirements.
- Percentage of EPA data in transit in compliance with encryption requirements.
- Percentage of "Zero Trust Architecture" projects completed on time.
- Implementation of advanced event logging requirements (EL3) across EPA networks.

Goal Number/Objective: Cross-Agency Strategy 3

NPM Lead: Office of Mission Support (OMS)

1a. Purpose of Long-Term Performance Goal:
The intent of reporting on this long-term performance goal (LTPG) is to monitor the progress of implementing the requirements laid out in Executive Order (EO) 14028.

Once complete, EPA will be in compliance with five of the high priority directives from EO 14028. Compliance with the directives will emphasize information security and strengthen EPA's information technology infrastructure and increase resilience and resistance to malicious cyber-attacks.

There will be five annual performance goals related to this long-term performance goal, each relating to a distinct directive from the executive order. Progress towards completing each of these performance measures will convey a sense of increasing cybersecurity preparedness.

1b. Performance Measure Term Definitions:
System: Typically means an information system used or operated by an agency or by a contractor of an agency, or by another organization on behalf of an agency.

Multifactor Authentication (MFA): A mode of accessing a system that requires two means of identity verification for the user. The typical means are a unique password only known to the user and an identification badge only possessed by the user. Other means occasionally used for MFA are a random string of numbers which only the user and system can produce or biometric data specific to the user.

Zero Trust Architecture: Refers to a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

Data at Rest: Refers to any data that are kept on computer data storage. The data can be stored in many formats and on many different mediums.

Data in Transit: Refers to any data that are in route between origin and destination within a network.

Encryption: Refers to the conversion of data from an easily accessible and readable format into one where a key must be possessed to access and understand the data. This makes unauthorized use of data more difficult and ensures that merely gaining access to a network does not give an individual access to the information on the network.

Logging: Refers to the recording of the events occurring within an organization's systems and networks. Logs are composed of entries, and each entry contains information related to a specific event that has occurred within a system or network.

1c. Unit of Measure:
Each annual performance goal will have its own specific unit of measure to monitor and track results.

- MFA performance will be monitored with the percentage of systems in compliance with the Multifactor Authentication Requirements.
- Data at Rest (DAR) performance will be monitored by the percentage of physical and virtual servers in which the data stored has been encrypted.
- Data in Transit (DIT) performance will be monitored by the percentage of networks which only allow encrypted traffic.
- Zero Trust Architecture (ZTA) performance will be monitored by the establishment of a Zero Trust Architecture project roadmap, and the completion of identified projects.
- Advanced Logging Requirements (ALR) performance will be monitored by tracking the logging requirements across EPA networks according to a predetermined set of maturity levels.

2a. Data Source:
The data source will be collected in EPA's information systems. The data are provided by the Office of Information Security and Privacy and supporting regions and national programs.

2b. Data needed for interpretation of (calculated) Performance Result:
As of FY 2023, 79% of EPA's systems have implemented multi-factor authentication; 21% of systems have yet to implement multi-factor authentication. EPA's networks are currently at the EL0 level for logging requirements.

3. Calculation Methodology:
Performance results will vary depending on the annual performance goal. There will be percentages which will take the number of completed portions of a performance measure divided by the total number of portions required for completion. The performance results for the logging requirement measure will be calculated by using a set scale.

4. Quality Assurance/Quality Controls:
TBD

5. Data Limitations/Qualifications:
A potential source of error in reporting on these annual performance goals is the possibility that the collection of networks or systems which are being targeted could change. This impact would be slight, however, the overall monitoring of this initiative will not be affected by changes to which systems are being worked on.

The completion of this long-term performance goal does not mean EPA has completed all cybersecurity tasks. The nature of cybersecurity is dynamic and evolving and requires constant monitoring and updating as threats change and the demands of users grow. Ongoing maintenance and monitoring will be required beyond the implementation of this long-term performance goal.

6. Technical Contact:
Mark Bacharach (OMS), Deputy Office Director, Office of Information Security and Privacy, 202-566-2950

7. Certification Statement/Signature:

I certify the information in this DQR is complete and accurate.

DAA Signature Original signed by Vaughn Noga **Date** 1/30/2024