

Binding Operational Directive 23-01

Compliance Guide

By April 3, 2023, all FCEB agencies must deploy an updated CDM Dashboard configuration that enables access to object-level vulnerability enumeration data for CISA analysts. Agencies must demonstrate their ability to:

- ✓ Perform automated asset discovery of all IP-addressable assets every 7 days
- ✓ Initiate vulnerability enumeration every 14 days
- ✓ Upload vulnerability results into the Continuous Diagnostics and Mitigation (CDM) Agency Dashboard within 72 hours
- ✓ Initiate asset discovery and vulnerability on demand as required within 72 hours



Asset Risk Management and BOD 23-01 Controls

Sepio’s Asset Risk Management (ARM) platform is a SaaS or on-premise solution that provides a new dimension of complete asset visibility. Our patented technology harnesses immutable properties at the physical layer to objectively identify every known and shadow asset, regardless of its functionality or operability, on a continuous basis. This unique approach means Sepio is untainted by misleading profile perceptions and behavioral assumptions that can deceive even the most robust cyber tools. With its agnostic visibility, Sepio protects federal entities’ Cyber Physical Systems which encompass a variety of interconnected IT, OT and IoT assets.

Sepio generates an Asset Risk Factor (ARF) score for every device in real-time, prioritizing those that impact business continuity and alerting on risks so security teams instantly understand what needs attention. In doing so, enterprises expedite time to resolution, identify regulations gaps and prevent crises. The platform is augmented by OSINT data sources and internal cyber research to provide up-to-date threat intelligence vulnerability enumeration for all assets, further optimizing IT efficiency.

As a trafficless solution, Sepio is infinitely scalable to protect the entire asset infrastructure as fast and often as anyone, anywhere connects any assets to the entity’s decentralized, uncontrolled ecosystem. With Sepio providing a centralized, holistic and reliable source of truth, federal agencies can confidently meet CISA’s requirements.

BOD 23-01 Controls and Sepio

BOD 23-01 Control	Support from Sepio
Perform automated asset discovery every 7 days	Sepio’s trafficless asset discovery approach sees all known, shadow and rogue assets as soon as they are connected, wherever they are, whoever installed them, however they are or aren’t in use, providing an up-to-date inventory of all assets within the scope of BOD 23-01 – IT/OT/IoT
Initiate vulnerability enumeration every 14 days	Sepio continuously scans the entire IT/OT/IoT asset infrastructure for existing vulnerabilities
Upload vulnerability results into the Continuous Diagnostics and Mitigation (CDM) Agency Dashboard within 72 hours	Sepio’s extensive reporting capabilities easily drive automation processes independently or through its detailed API into the CDM dashboard
Initiate asset discovery and vulnerability on demand as required within 72 hours	Sepio continuously scans the entire IT/OT/IoT asset infrastructure to provide the most up-to-date asset inventory with enumerated vulnerabilities. Furthermore, an immediate on-demand scan can be initiated through Sepio’s dynamic scanning settings