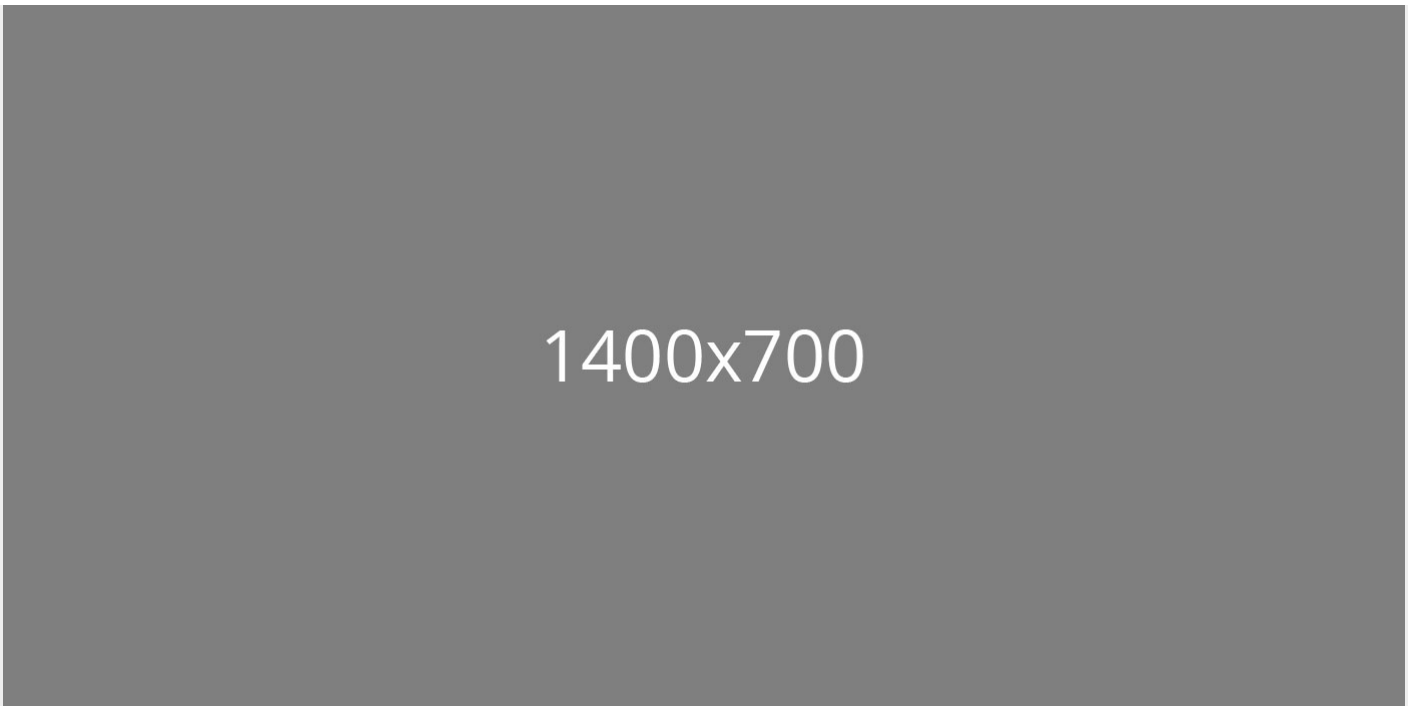
ACHIEVE COMPLIANCE FOR CISA'S BINDING OPERATIONAL DIRECTIVE 23-01 WITH BMC



The United States Cybersecurity and Infrastructure Security Agency (CISA) released the Binding Operational Directive 23-01, a compulsory directive to the federal, executive branch, departments, and agencies to safeguard federal information and information systems. Under the directive, agencies must have weekly automated asset discovery and vulnerability enumeration in place by April 3, 2023.

Federal agencies are embracing the challenge of managing and securing hardware and software assets across multi-cloud, on-premises, and mobile. This complexity comes with increased cybersecurity risk. One way organizations can manage this risk is through continuous and comprehensive asset visibility. Maintaining accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian Executive Branch (FCEB) enterprise.

The new requirements

Binding Directive 23-01 focuses on two core areas:

- **Asset discovery** as a building block of operational visibility, defined as an activity through which an organization identifies the network-addressable IP assets that reside on its networks and their associated IP addresses (hosts).
- **Vulnerability enumeration** identifies and reports suspected vulnerabilities on those assets. It detects host attributes (e.g., operating systems, applications, open ports, etc.) and attempts to identify outdated software versions, missing updates, and misconfigurations. It validates

compliance with or deviations from security policies by identifying host attributes and matching them with information on known vulnerabilities.

BMC answers the call

You can't manage what you can't see. Below are the ways that BMC Helix Discovery, a FedRAMP Moderate-certified, SaaS solution delivered on Amazon Web Services (AWS), can help you meet the Binding Operational Directive 23-01 requirements:

Requirement	BMC Helix Discovery
Maintain an up-to-date inventory of networked assets	Inventories networked hardware and software assets across cloud, hybrid, and on-premises environments. Adds the additional benefit of relationship/dependency mapping and service modeling.
Perform automated asset discovery every seven days	Agentless discovery of assets with automated scheduling at any interval (hourly, daily, weekly, etc.)
Initiate vulnerability enumeration across all discovered assets, including all discovered nomadic/roaming devices, every 14 days	Completely catalogs asset configurations and profiles for vulnerability enumeration at every scan
Develop and maintain the operational capability for on-demand asset discovery and vulnerability enumeration to identify specific assets or subsets of vulnerabilities within 72 hours of CISA request and provide results within seven days	Can be executed on-demand to meet CISA requests and immediately provides results
Perform the same type of vulnerability enumeration on mobile devices and other devices that reside outside of an agency's on-premises networks	Treats mobile devices and other offsite devices, including tablets, iOS and Android devices, the same as on-premises networked assets

BMC Helix Discovery provides real-time visibility into hardware and software assets as well as their relationships and service dependencies across on-premises and cloud environments. It is designed to handle the complexity of managing a wide spectrum of configurations, including physical and logical components. Learn more about what BMC Helix Discovery can do to help your agency meet CISA's Binding Operational Directive 23-01 requirements. Reach out to federal@bmc.com, speak to your BMC Account Team, or visit www.bmc.com/discovery.