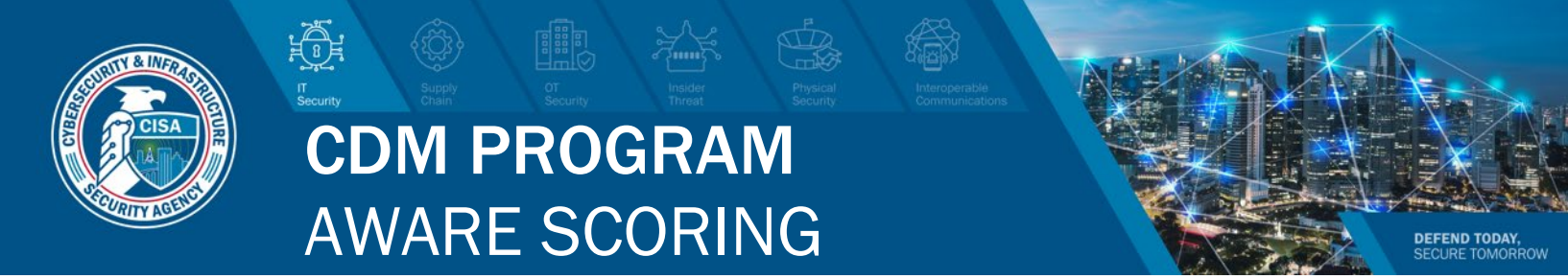

CDM PROGRAM
AWARE SCORING

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow. The Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of civilian government networks and systems.

AWARE OVERVIEW

Agency-Wide Adaptive Risk Enumeration (AWARE) answers the need for a standardized attack surface scoring methodology across the federal civilian enterprise that provides situational awareness of security posture by considering defect type, how long the defect has existed, whether the defect occurs on a system of high value, and other critical factors. CISA's CDM Program created AWARE by combining key aspects of federal attack surface scoring systems used by the Department of State's continuous monitoring and risk reporting application (iPost) and the Department of Justice's Security Posture Dashboard Report. AWARE was developed in partnership with federal civilian agencies participating in the CDM Program. As needs change and technologies evolve, the CDM Program will continue using agencies' insight to enhance AWARE and improve CDM capabilities.

BENEFITS OF AWARE SCORING

Through prioritization, AWARE encourages timely remediation of security exposure while improving an organization's ability to manage the attack surface effectively. Defects that represent the highest risk exposure are prioritized on an organization's CDM Agency Dashboard. The AWARE score is "configurable" because it considers the potential consequences of defects (e.g., system criticality) and the likelihood of threats posed (e.g., based on CISA threat intelligence and commercial threat feeds) while also emphasizing situational awareness and creating integrated outputs that yield an actionable picture of attack surface posture for stakeholders.

AWARE SCORING DETAILS

Scores associated with specific defects are categorized under three distinct factors.

- **Software Vulnerability (VUL)** – Consists of individual Common Vulnerability and Exposures (CVEs) identified on network endpoints by VUL scanning tools during Asset Management.
- **Configuration Settings Management (CSM)** – Defects that fail a CSM check carried out by CSM tools are scored by assigning a scaled value within the Common Vulnerability Scoring System (CVSS) scale based on severity.
- **Unauthorized Hardware (UAH)** – UAH represents hardware devices that have not been assigned ownership in a dashboard container. Unassigned assets are discovered using Hardware Asset Management tools during Asset Management discovery.

AGENCY-WIDE ADAPTIVE RISK ENUMERATION (AWARE)

AWARE assigns scores for the VUL, CSM, and UAH factors based on the intersection of four metrics.

- **Base** – Starts with base CVSS value, then applies logarithmic scaling to prioritize the worst problems first.
- **Age** – Measured from the publication date of a CVE, with 90 days to double score from base CVSS; encourages timely remediation of vulnerabilities.
- **Weight** – Includes two independent factors:
  - *Federal Vulnerability Action* – Weight factor affecting a CVE due to a heightened threat level for that CVE as informed by threat intelligence.
  - *High Value Factor* – Weight factor that occurs on endpoints in FISMA systems with a Federal Information Processing Standard Publication 199 impact of "high."
- **Allowable Tolerance** – Intended to give agencies time to test and deploy patches or mitigate vulnerabilities before the agency's federal score is impacted; it begins when a vulnerability is added to the Agency Dashboard.

AWARE Score = Scaled Base CVSS [Vulnerability] X Age X Weight [Threat, Impact] X Tolerance [Grace Period]

TIMELINE

Agencies should be using their AWARE results now to make decisions and address their worst problems first. Agencies should hold themselves accountable for AWARE results. DHS encourages agencies to use their federal average score (available in AWARE with Release 6 of the Agency Dashboard) to assess their cybersecurity posture in comparison to other agencies across the .gov.