wiley

ALERT

CISA Directive Highlights Risk-Based Vulnerability Management

June 10, 2026

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a new Binding Operational Directive to federal agencies that updates vulnerability management processes and instructs agencies to prioritize security updates based on risk. Binding Operational Directive (BOD) 26-04, *Prioritizing Security Updates Based on Risk*, was issued June 10, 2026, along with related implementation guidance that CISA intends to update on a rolling basis.

The directive applies to federal civilian Executive branch agency information systems, and while it does not apply to federal contractors, CISA has directed those agencies to review contracts to ensure that contractors who support or operate agency information systems can ensure agency compliance with the directive. According to CISA, the guidance is intended to focus "patching efforts on the areas of highest risk rather than treating all vulnerabilities and systems equally" – and, notably, assigns timelines as short as three days for implementing patches.

Key Takeaways

- The directive provides a method for agencies to prioritize security updates based on a risk assessment. Such methodology may be useful for commercial businesses as well as government agencies.
- CISA offers aggressive, bordering on unrealistic, timelines. Companies should understand that there are potential risks that this guidance will be misunderstood to establish a patching schedule that all organizations should follow.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Erin M. Joe
Special Counsel
202.719.3140
ejoe@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement
Cybersecurity
Emerging Technologies
Government Contractors & Grantees
Government Contracts
Privacy and Cybersecurity Litigation and Investigations
Privacy, Cyber & Data Governance
Trump Administration Resource Center

- Government contractors may see requirements extended beyond government agencies and may anticipate government contracting officers including these requirements in Statements of Work and future contracts.
- Cloud Service Providers may plan to adopt these requirements in anticipation of likely updates to government contracts and, potentially, FedRAMP requirements.

What the Directive Does

CISA intends BOD 26-04 to ensure that agencies make remediation decisions using a consistent framework for prioritizing software updates. Rather than treating every vulnerability as equally urgent, the directive requires agencies to assess four factors: 1) whether the vulnerable asset is publicly exposed; 2) whether a vulnerability is known to be exploited; 3) whether an adversary can automatically exploit the vulnerability; and 4) whether the exploitation offers an adversary "partial" or "total" control of a vulnerable asset. CISA provides some guidance for agencies on how to determine whether a vulnerability can be automatically exploited, and how much control an adversary can obtain, but in practice, this information may be incomplete or difficult for an organization to verify. The guidance also does not address situations in which vulnerabilities are "in the wild" before they've been incorporated into the Known Exploited Vulnerability (KEV) catalog, nor does it address vulnerabilities for which no patch is available.

CISA also directs agencies to implement the directive by updating their vulnerability management policies and using CISA-provided capabilities for automated vulnerability reporting and network scanning. The associated implementation guidance provides additional details on how agencies should perform the required forensic triage, and addresses "frequently asked questions" (FAQs).

Within 180 days (by December 7, 2026), agencies are directed to adopt an aggressive timeline for vulnerability remediation: A vulnerability that meets all four risk factors because it offers total control of a publicly exposed device, can be automatically exploited, and is in the Known Exploited Vulnerability database, must be remediated within three days, and the agency must perform "forensic triage" to assess whether the vulnerability has been exploited on the given system. To be clear, a three-day deadline is extremely aggressive and assumes that a patch or mitigation already exists that can be applied to the given system and is documented in the CISA-supported KEV catalog. CISA's FAQs suggest that implementing the specific available patch is the default remediation, and instruct agencies to contact CISA for "special use cases" that might cause "severe difficulty implementing a specific patch."

Why This Matters

For contractors and private-sector organizations, the CISA directive is noteworthy because federal cybersecurity expectations often influence contractual requirements, procurement expectations, and broader market practice. Organizations that support federal environments may therefore want to revisit how they assess patching priorities, exception handling, and document remediation decision-making. We also expect that contractors who provide information systems to federal civilian agencies will start to see updates from their contracting officers to incorporate changes to their Statements of Work to address these new

requirements.