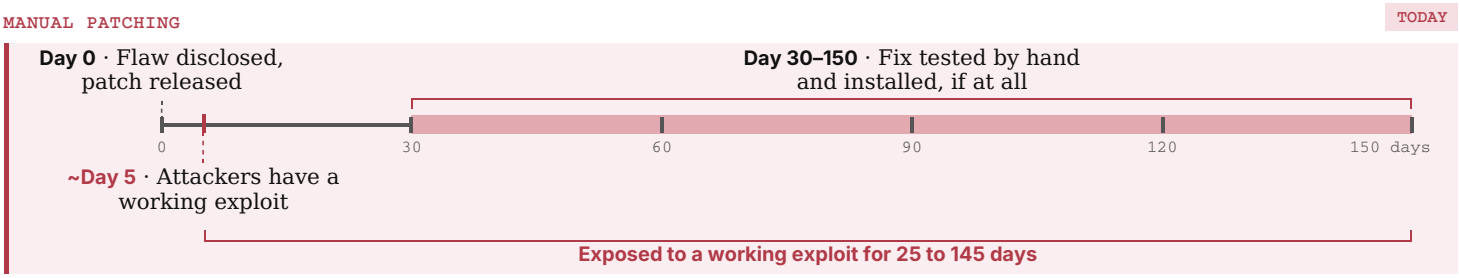
UNITED STATES CONGRESSMAN
GEORGE WHITESIDES
REPRESENTING THE 27TH DISTRICT OF CALIFORNIA

Cyber Resilience for Critical Infrastructure Act

AI is collapsing the time it takes attackers to exploit a known flaw, while the utilities, hospitals, and water systems Americans depend on still take months to install the fix. This bill funds the **tools** that make fast patching safe, helps operators **wall off** systems that can't be patched quickly, and gives every sector a clear, realistic benchmark for what "fast enough" means.

The Problem, In One Timeline

A critical vulnerability in industrial control software is publicly disclosed.



Testing is manual, maintenance windows are narrow, and staff are thin. Patches are deployed only ~58% of the time.

What The Bill Does

A clear definition of "fast enough"

NIST publishes a cross-sector baseline within 6 months, then patching benchmarks for energy, water, healthcare, and communications within 9 months and all other sectors within 15. Benchmarks account for real-world limits like downtime tolerance, safety risks, and device certification. Where patching isn't practical, isolating a system from the internet counts as an alternative.

Funding to patch faster, or wall systems off

CISA, with FEMA, awards competitive grants for automated patch deployment, safe testing environments, and asset inventories. For systems that can't be patched quickly, grants fund network segmentation, cutting operational technology off from the internet, and replacing outdated edge devices. Operators without IT staff can use funds for managed services.

Most help for those least able to pay

The federal government covers 100% of project costs for small, rural, and municipal operators and state and local entities, 75% for mid-size operators, and 50% for large companies. Separately, 30% of all grant dollars are reserved for small, rural, and municipal operators. Entities with over $10 billion in revenue are ineligible.

Accountability without exposure

Grantees commit to meeting their sector benchmark and report each year how fast they fix actively exploited vulnerabilities or how many systems they've taken off the internet. Contractors must follow recognized security practices. Reports are aggregate only and protected from public disclosure and regulatory enforcement.

Funding

- **$250 million over five years**, modeled on existing energy-sector cybersecurity grant programs.
- **Measured results.** NIST and CISA report to Congress at two years on whether grantees are patching faster and reducing internet exposure compared with their sectors.

What It Does NOT Do

- Does not impose any patching mandate. Benchmarks are voluntary and apply only to operators who accept grant funds.
- Does not require rulemaking or create new regulatory penalties.
- Does not claw back funds from grantees who miss a milestone in good faith.
- Does not require operators to disclose specific vulnerabilities or systems.
- Does not fund general IT upgrades, incident response, or insurance, or favor any vendor.