



National Cybersecurity Awareness Month: DoW's “Brilliant at the Basics” for IT and OT

Public paper · October 3, 2026 · General desk · Ryan Standley / Record of Sale, LLC / Notice Nearby

A plain-language brief on the October 2, 2026 White House message for National Cybersecurity Awareness Month, and on the Department of War Chief Information Officer campaign that lists ten IT basics and ten OT basics for defense industry partners.

October is National Cybersecurity Awareness Month. On October 2, 2026, the White House issued a presidential message on the month. The Department of War (DoW) Chief Information Officer (CIO) is running a related campaign called “Brilliant at the Basics.” The campaign page is written for Defense Industrial Base partners. A public note from the DoW CIO also names warfighters, the civilian workforce, and that industrial base, and it covers both information technology (IT) and operational technology (OT).

This short brief reports what those sources say. It does not take a political side, and it does not add facts that are not in them.

What Awareness Month is about

The White House message calls cyberspace a frontier of American innovation, prosperity, and strength. It says a secure cyberspace matters for leadership in finance, military power, emerging technology, and manufacturing, and that freedom and security online cannot be taken for granted. It says adversaries and cybercriminals long targeted citizens, communities, and businesses, and that the administration has ended what it calls an era of weakness. This brief repeats that line as written. It does not grade it. The DoW CIO public note ties the month to work for warfighters, civilian employees, and defense industry partners, on both IT and OT.

What the White House message says

The message lists steps the administration says it has taken. The president signed an executive order to combat cybercrime, fraud, and predatory schemes, and to stop foreign criminal networks from preying on vulnerable Americans. The message does not give that order's number or full title, so this brief does not add one.

In March, the president released a Cyber Strategy for America, described as a vision for cybersecurity and innovation. The message says that strategy is already moving through "GOLD EAGLE," a partnership between the federal government and leading American companies. Its stated job is to use American Super Intelligence to find cybersecurity vulnerabilities quickly, stay ahead of adversaries, defend the public from new threats, and protect critical infrastructure tied to national security and competitiveness. "Super Intelligence" is the White House's term.

The message also points to the next generation. It credits First Lady Melania Trump's leadership of the Presidential Super Intelligence Challenge, which it says has encouraged young Americans to use new technology, learn skills, and solve problems in their communities. It names her Fostering the Future Together initiative, which it says helps students, parents, and educators learn through the safe and innovative use of advanced technology.

For the public, the message offers three habits: create strong passwords, keep software up to date, and stay alert to scams.

What "Brilliant at the Basics" is

The campaign is for small, mid-sized, and non-traditional Defense Industrial Base companies. The page says the mission is to help them secure networks, protect sensitive Department of War information, and deliver what it calls peace through technical strength. IT covers office computers, accounts, and business networks. OT covers systems that run physical equipment, including robotic arms, SCADA controls, and weapon systems, where downtime is often not an option. The two top-ten lists are published basics for partners. They are not, by themselves, a new statute.

IT basics in plain English

The IT ten, in everyday words, start with sign-in and housekeeping. Use phishing-resistant multi-factor authentication, not text-message codes or simple push alerts, and give people only the access their job needs. Keep a living inventory of hardware, software, identities, and data. Cut technical debt by retiring unused systems, extra data stores, unsupported software, and needless connections. The page says unmanaged "shadow IT" is an easy target. Prefer open standards so the company is not locked to one vendor.

Then limit how far a break-in can travel. Split the network into zones. The page calls that limiting the blast radius. Fix vulnerabilities that are actually exploitable in your setup, not only those with a high generic score. Build security into software early, including scans of third-party parts. Do not put sensitive department data into public commercial artificial-intelligence tools; use filters, endpoint controls, and approved company tools instead. Keep backup copies an attacker on the main network cannot change or delete, use separate login secrets, practice a full restore, and keep training the technical staff.

OT basics in plain English

The OT ten follow the same idea on the plant floor. Check identity, require multi-factor authentication on sensitive systems, and grant least privilege. The page calls this "never trust, always verify." Inventory what is really running: controllers, remote terminal units, operator screens, engineering workstations, control systems,

and safety systems, plus versions, protocols, programs, temporary gear, and remote links. Confirm that list with quiet monitoring and walk-throughs. Separate business IT from operational systems.

Plan for trouble without assuming a full shutdown is safe. The page says life safety, the environment, and keeping machines available come first. Keep offline backups, keep safety systems separate, work with vendors, and rehearse with cyber staff and process engineers. If a machine cannot be patched now, use compensating controls such as firewall rules, isolation, and allow-lists until maintenance. Open remote access only briefly, with strong authentication, and avoid always-on links, including gear exposed to the internet.

Watch production-floor logs, because you cannot stop what you cannot see. Design systems to fail safely, with redundancy and manual overrides. Hold suppliers to the same security standard, ask that new systems meet Department of War standards before purchase, and schedule replacement of hardware that cannot be defended. Review every significant change, including security updates, so a fix does not create an unsafe condition.

What readers can do

Members of the public can follow the three habits in the White House message: strong passwords, updated software, and care around scams.

A small or mid-sized company that handles Department of War information can start with the campaign checklist: phishing-resistant sign-in, a real inventory, network separation, backups that have actually been restored, and a rule that sensitive department data stays out of public AI chats.

Warfighters and civilian defense employees are named in the department's public note for the month. The ten-and-ten lists are written for industry partners. People inside the department should follow their own component's rules. This brief does not replace those rules, and it is not security consulting or legal advice.

Sources

White House, Presidential Message on National Cybersecurity Awareness Month, October 2, 2026: <https://www.whitehouse.gov/briefings-statements/2026/10/presidential-message-on-national-cybersecurity-awareness-month/>

Department of War Chief Information Officer, Brilliant at the Basics: <https://dowcio.war.gov/BrilliantBasics/>

Department of War Chief Information Officer public post on the month, naming warfighters, the civilian workforce, and the defense industrial base, for IT and OT:
https://x.com/DoW_CIO/status/2106353769449492794

Notes

- Facts from the White House presidential message of October 2, 2026, and from the Department of War Chief Information Officer "Brilliant at the Basics" page. The line on warfighters, the civilian workforce, and the defense industrial base is from the DoW CIO public post cited above.

- "Super Intelligence" is the White House message's term. This brief does not rename it.

- Author: Ryan Standley / Record of Sale, LLC / Notice Nearby.

- Discussed on @NoticeNearYou: (pending — fill xPostUrl after live post).

- Not legal advice. Not a newspaper. Not Legal Publication. Record of Sale, LLC (Oregon).

General desk · Notice Nearby public papers shelf. @NoticeNearYou post pending.

noticenearby.com/papers/cyber-awareness-brilliant-basics-oct-2026