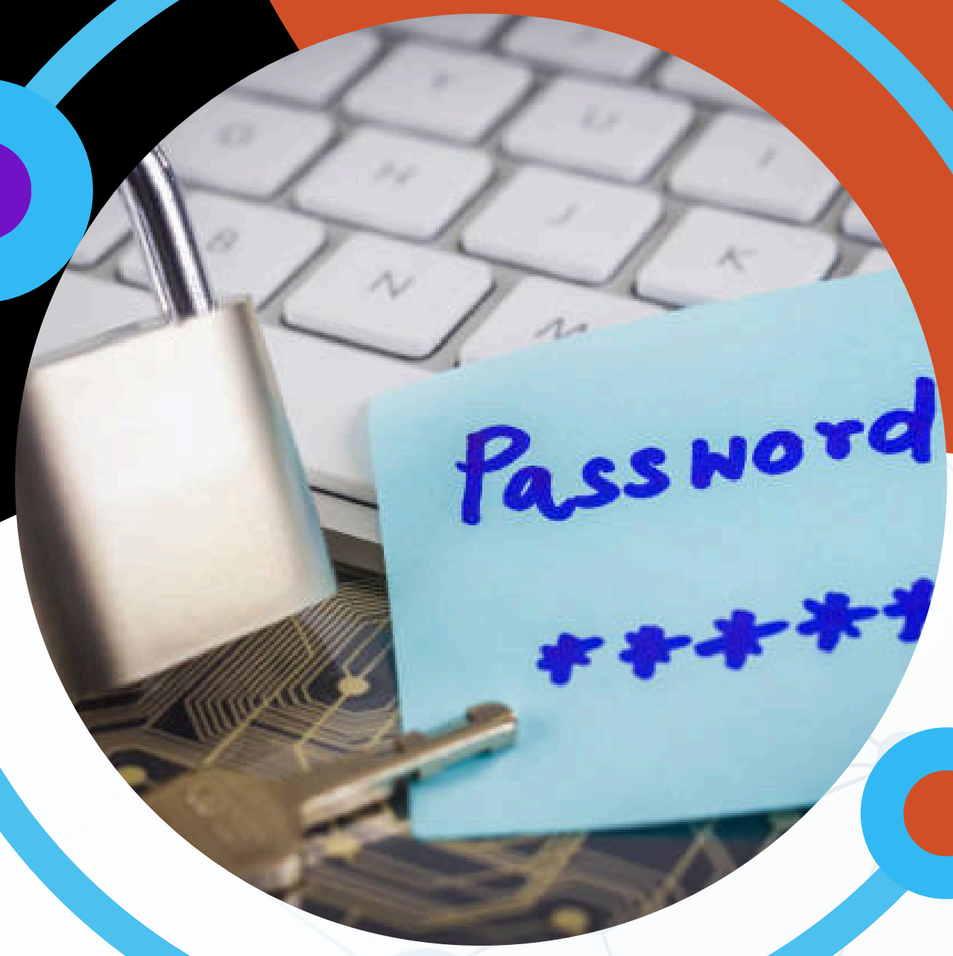
LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

JUNE 2026



CUI: PREVENTING UNAUTHORIZED DISCLOSURE

Controlled Unclassified Information (CUI) is sensitive government related information that requires safeguarding but is not classified. Employees across the workforce are responsible for properly handling, storing, transmitting, and destroying CUI in accordance with established procedures and government requirements. Unauthorized disclosure of CUI can damage operations, compromise privacy, create contractual issues, and increase risk to national security. Many disclosures are unintentional, but even accidental exposure can have serious consequences.
Protecting CUI depends on awareness, accountability, and consistent security practices.

Understanding Unauthorized Disclosure

Unauthorized disclosure occurs when CUI is shared with individuals who do not have authorized access or a lawful government purpose. This may occur through improper email transmission, unsecured storage, accidental conversations, or use of unauthorized systems or devices.

Examples include sending information to the wrong recipient, leaving documents unattended, discussing sensitive matters in public areas, or uploading files to unapproved platforms.

Employees should remain mindful of their surroundings and exercise caution whenever handling sensitive information.

Why CUI Protection Matters

Although CUI is not classified, it still requires protection. CUI may include information related to contracts, operations, personnel, cybersecurity, or proprietary data. Unauthorized disclosure can negatively affect mission operations, business relationships, and public trust.

Adversaries may attempt to collect CUI because it can provide insight into government activities or vulnerabilities.
Protecting CUI supports operational security and national security objectives.

Common Causes of Unauthorized Disclosure

Many unauthorized disclosures result from everyday mistakes rather than malicious intent. Common causes include failure to verify email recipients, improper document marking, weak password practices, unsecured meetings, and discussing sensitive information in unauthorized environments.

Remote work and digital collaboration have increased opportunities for accidental exposure.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

Security awareness and attention to detail remain essential safeguards.

Best Practices for Protecting CUI

Employees can help prevent unauthorized disclosure by following established handling procedures and maintaining strong security habits. This includes properly marking documents, verifying recipients before transmitting information, using approved systems, and securing workspaces.
CUI should only be shared with authorized individuals who have a lawful government purpose and a need to know.
Consistent security practices reduce risk and help protect sensitive information.

Reporting and Accountability

Prompt reporting is critical when unauthorized disclosure is suspected or confirmed. Early reporting allows Security personnel to assess the situation and contain potential damage.

Employees should immediately report lost devices, misdirected emails, suspected compromise, or possible unauthorized access to CUI.

Protecting sensitive information requires accountability from every employee.

If You See Something, Say Something

If you observe possible mishandling or unauthorized disclosure of CUI, report it through appropriate security channels immediately.

Protecting CUI protects the mission, the organization, and national security.

References:

- National Archives and Records Administration (NARA). Controlled Unclassified Information Program. https://www.archives.gov/cui
- Defense Counterintelligence and Security Agency (DCSA). Controlled Unclassified Information (CUI) Guidance. https://www.dcsa.mil/

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com