DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CHIEF OF NAVAL TRAINING
SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION

Ref: (a) DOD M-5200.01, Volume 4
(b) DEPSECDEF Memo of 14 Aug 14

1. It is the policy of the Chief of Naval Air Training (CNATRA) that all authorized Naval Air Training Command (NATRACOM) users of DoD information systems, and those with access to Controlled Unclassified Information, understand and comply with policy and guidance provided in references (a) and (b) to prevent unauthorized disclosures. In addition to classified information, certain types of unclassified information in the custody and control of NATRACOM activities require application of access and distribution controls and protective measures. Controlled Unclassified Information (CUI) is a term that encompasses a wide range of information categories, to include Personally Identifiable Information (PII), law enforcement sensitive information, proprietary commercial or financial information received on a privileged basis, information related to physical security or protected critical infrastructure, export-controlled information, etc. If released, such information may pose a threat to security and to DoD operations and missions. All DoD unclassified information must be properly reviewed and approved for release through normal processes before it is provided to the public, to include via posting to publicly accessible websites.

2. CNATRA Department Heads/Special Assistances and NATRACOM Commands are to familiarize themselves with the types of CUI within their organization, and institute effective safeguards with respect to the handling, storage, and dissemination of such CUI. Where dissemination of CUI is required in the conduct of official DoD business, all personal will ensure that such dissemination is consistent with any and all controls specifically applicable to such information. When transmitting electronically, utilize only approved secure communication systems and/or appropriate protective measures (e.g., encryption). Ensure recipients of CUI are properly informed of the nature of information being transmitted, and any handling requirements and restrictions.

3. Data owners are responsible to ensure that CUI data stored on electronic devices (e.g., File Servers, Shared Drives, and External Storage Devices) are properly protected with encryption and access permissions. Only users with the need to view or access the files should be given permissions. Users who no longer need the access should be removed immediately. In instances of unauthorized disclosures of CUI, notification will be immediately made to the CNATRA Security Manager. Data spillages and unauthorized disclosures must be aggressively monitored, and commanders and supervisors at all levels shall investigate and, when they deem appropriate, take appropriate administrative and/or disciplinary actions with respect to those who are found to have caused or contributed to such incidents. Commanders and supervisors will, as they deem appropriate, suspend user accounts for willful violations or while corrective actions are pending.

4. Training on protection of CUI will be incorporated into NATRACOM indoctrination briefings, as well as annual information assurance briefs. Refresher training may be ordered, as necessary, in response to incidents. Work center supervisors are to ensure that members, employees, and contractors handling CUI are properly trained on specific procedures related to the specific marking, storage, and dissemination controls.

G. N. HARRIS