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

CNATRAINST 5570.1
N00
11 June 2018

CNATRA INSTRUCTION 5570.1

Subj: SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

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

Encl: (1) CUI OF901 Coversheet
(2) PII Coversheet DD Form 2923

1. Purpose. To promote awareness and promulgate policies within the Naval Air Training Command (NATRACOM) regarding protection of unclassified information, the release of which may pose a threat to security and to DoD operations and missions. All authorized users of DoD information systems, and those with access to Controlled Unclassified Information (CUI), must understand and comply with policy and guidance to prevent unauthorized disclosures.

2. Scope. In addition to classified information, certain types of unclassified information that are in the custody and control of NATRACOM activities require application of access and distribution controls and protective measures. Such information is generically referred to as CUI. Examples of CUI include:

a. Information that may be exempt from release under the Freedom of Information Act (FOIA);

b. "Law Enforcement Sensitive" materials;

c. Proprietary commercial or financial information provided from a non-Federal entity on a privileged basis;

d. Personally Identifiable Information (PII);

e. Information related to physical security and Protected Critical Infrastructure;

f. DoD Unclassified Controlled Nuclear Information;

g. Department of State information designated as "Sensitive but Unclassified";

h. Imagery or geospatial information and data designed by the National Geospatial-Intelligence Agency as "LIMITED DISTRIBUTION";

i. Information generated by NATO member countries and designated as "NATO Restricted" or "NATO Unclassified";

j. Information received from a Foreign Government marked "RESTRICTED" or otherwise on the condition that it will be treated in confidence."

This is only a representative sampling.

3. Policy

a. 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.

b. Chief of Naval Air Training (CNATRA) Department Heads/Special Assistances and NATRACOM Activity Heads are to familiarize themselves with the types of CUI within the custody and control of their organization, and to institute effective safeguards with respect to the handling, storage, and dissemination of such CUI.

c. Access to CUI will be limited to only those military members, civilian employees, and/or contractors that have a valid need for such access.

d. Where required by the particular type of CUI, ensure markings are properly annotated.

e. 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 that recipients of CUI are properly informed of the nature of the information being transmitted, and any handling requirements and restrictions.

f. Data Owners are responsible to ensure that CUI data stored on electronic devices (e.g. File Servers, Shared Drives, External Storage Devices) are properly protected with encryption and access permissions. Only users with the necessity to view or access the files should be given permissions. Users who no longer need the access should be removed immediately by the Data Owner.

g. When in receipt of a FOIA or other request for DoD information that is not generally releasable to the public, all personnel will immediately inform appropriate supervisors and notify the CNATRA Legal Office.

h. 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.

i. Data Owners are responsible for correct destruction of CUI. CUI must be destroyed to a degree that makes the information unreadable, indecipherable, and irrecoverable.

4. Training. 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 specific CUI are properly trained on specific procedures related to the specific marking, storage, destruction, and dissemination controls.

5. Review. In that CUI policy continues to develop within the Executive Branch and the DoD, the CNATRA Chief Information Officer, CNATRA Security Manager, and CNATRA Office of Counsel will review this instruction annually.

S. B. STARKEY
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

901-101
NSN-7540-01-633-7021

OPTIONAL FORM 901 (08-14)
Prescribed by GSA/ISOO | 32 CFR 2002

CONTROLLED

Privacy Act Data Cover Sheet

To be used on all documents containing personal information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in CIVIL and CRIMINAL penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

Privacy Act Data Cover Sheet

DD FORM 2923, SEP 2010